Foundations and Trends™ in Communications and Information Theory

Volume 1 Issue 3, 2004

Editorial Board

Editorial Scope

Foundations and Trends™ in Communications and Information Theory will publish survey and tutorial articles in the following topics:

- Coded modulation
- Coding theory and practice
- Communication complexity
- Communication system design
- Cryptology and data security
- Data compression
- Data networks
- Demodulation and equalization
- Denoising
- Detection and estimation
- Information theory and statistics
- Information theory and computer science
- Joint source/channel coding
- Modulation and signal design
- Multiuser detection
- Multiuser information theory
- Optical communication channels
- Pattern recognition and learning
- Quantization
- Quantum information processing
- Rate-distortion theory
- Shannon theory
- Signal processing for communications
- Source coding
- Storage and recording codes
- Speech and image compression
- Wireless communications

Information for Librarians
Foundations and Trends™ in Communications and Information Theory, 2004, Volume 1, 4 issues. ISSN paper version 1567-2190 (USD 200 N. America; EUR 200 Outside N. America). ISSN online version 1567-2328 (USD 250 N. America; EUR 250 Outside N. America). Also available as a combined paper and online subscription (USD 300 N. America; EUR 300 Outside N. America).

Algebraic Number Theory and Code Design for Rayleigh Fading Channels

Frédérique Oggier

Institut de Mathématiques Bernoulli
École Polytechnique Fédérale de Lausanne
Lausanne 1015, Switzerland

Emanuele Viterbo

Dipartimento di Elettronica Politecnico di Torino
C.so Duca degli Abruzzi 24
Torino 10129, Italy

now

the essence of knowledge

Foundations and Trends™ in Communications and Information Theory

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
USA
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

Printed on acid-free paper

ISSNs: Paper version 1567-2190; Electronic version 1567-2328

Foundations and Trends™ in
Communications and Information Theory
Vol 1, No 3 (2004) 333-415

now
the essence of knowledge

Algebraic Number Theory and Code Design for Rayleigh Fading Channels

F. Oggier[1] and E. Viterbo[2] (*)

[1] *Institut de Mathématiques Bernoulli, École Polytechnique Fédérale de Lausanne, Lausanne 1015, Switzerland, frederique.oggier@epfl.ch*
[2] *Dipartimento di Elettronica Politecnico di Torino, C.so Duca degli Abruzzi 24, Torino 10129, Italy, viterbo@polito.it*

Abstract

Algebraic number theory is having an increasing impact in code design for many different coding applications, such as single antenna fading channels and more recently, MIMO systems.

Extended work has been done on single antenna fading channels, and algebraic lattice codes have been proven to be an effective tool. The general framework has been settled in the last ten years and many explicit code constructions based on algebraic number theory are now available.

The aim of this work is to provide both an overview on algebraic lattice code designs for Rayleigh fading channels, as well as a tutorial introduction to algebraic number theory. The basic facts of this mathematical field will be illustrated by many examples and by the use of a computer algebra freeware in order to make it more accessible to a large audience.

* This work was partly supported by CERCOM and FIRB-PRIMO.

Table of Contents

1

Introduction

Elementary number theory was the basis of the development of error correcting codes in the early years of coding theory. Finite fields were the key tool in the design of powerful binary codes and gradually entered in the general mathematical background of communications engineers. Thanks to the technological developments and increased processing power available in digital receivers, attention moved to the design of signal space codes in the framework of coded modulation systems. Here, the theory of Euclidean lattices became of great interest for the design of dense signal constellations well suited for transmission over the Additive White Gaussian Noise (AWGN) channel.

More recently, the incredible boom of wireless communications forced coding theorists to deal with fading channels. New code design criteria had to be considered in order to improve the poor performance of wireless transmission systems. The need for bandwidth-efficient coded modulation became even more important due to scarce availability of radio bands. Algebraic number theory was shown to be a very useful mathematical tool that enables the design of good coding schemes for fading channels.

These codes are constructed as multidimensional lattice signal sets

(or constellations) with particular geometric properties. Most of the coding gain is obtained by introducing the so-called *modulation diversity* (or *signal space diversity*) in the signal set, which results in a particular type of bandwidth-efficient diversity technique.

Two approaches were proposed to construct high modulation diversity constellations. The first was based on the design of intrinsic high diversity algebraic lattices, obtained by applying the *canonical embedding* of an *algebraic number field* to its *ring of integers*. Only later it was realized that high modulation diversity could also be achieved by applying a particular rotation to a multidimensional QAM signal constellation in such a way that any two points achieve the maximum number of distinct components. Still, these rotations giving diversity can be designed using algebraic number theory.

An attractive feature of this diversity technique is that a significant improvement in error performance is obtained without requiring the use of any conventional channel coding. This can always be added later if required.

Finally, dealing with lattice constellations has also the key advantage that an efficient decoding algorithm is available, known as the *Sphere Decoder*.

Research on coded modulation schemes obtained from lattice constellations with high diversity began more than ten years ago, and extensive work has been done to improve the performance of these lattice codes. The goal of this work is to give both a unified point of view on the constructions obtained so far, and a tutorial on algebraic number theory methods useful for the design of algebraic lattice codes for the Rayleigh fading channel.

This paper is organized as follows. Section 2 is dedicated to the communication problem. All the assumptions on the system model and the code design criteria are detailed there. We motivate the choice of lattice codes for this model.

Since some basic knowledge of lattices is required for the code constructions, Section 3 recalls elementary definitions and properties of lattices.

A very important feature to consider when designing codes is their decoding. Application of arbitrary lattice codes became attractive thanks to the *Sphere Decoder*, a universal lattice decoding algorithm, described in Section 4 in its original form.

Section 5 is a self-contained short introduction to algebraic number theory. It starts from the very elementary definitions, and focuses on the construction of *algebraic lattices*.

Section 6 introduces the key notion of *ideal lattice*, which gives a unifying context for understanding algebraic lattice codes. It allows the construction of close form expressions for the key performance parameters of lattice codes in terms of algebraic properties of the underlying number field.

At this point, we have all the mathematical tools to build efficient lattice codes. Some explicit constructions are given and their performance is shown in Section 7. Once again, the algebraic properties of the lattice will help us in deriving a bound on the performance, which we will use to show that known lattices codes are almost optimal, and that no significant further improvement can be achieved.

In Section 8, we give a brief overview of other applications of the theory of algebraic lattice codes; for instance, complex lattice codes can be used similarly to the real ones in the case where we assume complex fading coefficients. Finally, we give an example of algebraic space–time block code, to illustrate how this theory can be generalized and used in the context of cyclic division algebras for designing codes for MIMO channels. This last application is a promising area of research, and we give here an example to motivate further investigations.

For readers interested in implementing the constructions of algebraic lattice codes, we add at the end of Sections 5 and 7 some commands in KASH/KANT, a computational algebra software tool. In such a programming language, all the elementary algorithms for number field computations are readily available.

2

The Communication Problem

We start by detailing both the channel and the transmission system model that we consider. We then present the design criteria related to this model: *diversity* and *product distance*. Finally, we discuss how the labeling and shaping problems motivate the choice of particular lattice codes.

2.1 The Fading Channel Model

We consider a wireless channel modeled as an independent Rayleigh flat fading channel. We assume perfect *Channel State Information* (CSI) is available at the receiver and no inter-symbol interference is present. The discrete time model of the channel is given by

$$r' = \alpha' x + n'$$

where x is a symbol from a complex signal set, n' is the complex white Gaussian noise and α' the complex zero mean Gaussian fading coefficient. The complex fading coefficients are assumed to be independent from one symbol to the next. This assumption can be made reasonable by introducing a channel interleaver which breaks up the actual fading process correlations. Since CSI is available at the receiver, the phase φ

of the fading coefficient can be removed so that we get

$$r = \alpha x + n \tag{2.1}$$

where $\alpha = |\alpha'|$ is now a real Rayleigh-distributed fading coefficient and $n = n'e^{-i\varphi}$ remains the complex white Gaussian noise. In this case both in-phase and quadrature components of the transmitted symbol are subject to the same fading. In order to fully exploit the diversity capabilities of our codes, we will additionally introduce an *in-phase/quadrature component interleaver* which will enable us to consider the fading channel model in (2.1) where we assume that $x \in \mathbb{R}$, n is a real Gaussian random variable and the fading coefficients are independent from one real transmitted symbol to the next.

When considering coded transmissions, codewords will be n-dimensional real vectors $\mathbf{x} = (x_1, \ldots, x_n)$ taken from some finite signal constellation $S \subseteq \mathbb{R}^n$. Each vector component is assumed to be affected by an independent real fading coefficient. This is possible by implementing the modulator as follows (see Fig. 2.1). A pair of codewords is taken and the component interleaver swaps the quadrature components between the two codewords, as shown for example in Fig. 2.1(a). Then, a pairing of the components is done to build complex symbols (e.g., $x_1 + iy_2$), and each of them is sent over a time interval T (see Fig. 2.1(b)). Finally, the de-interleaver at the receiver restores the two initial codewords, which are now affected by real independent fading coefficients (see Fig. 2.1(c)). Note that the transmitted complex symbol (e.g., $x_1 + iy_2$) may not belong anymore to the original complex constellation of x.

Remark 2.1. The same model is also valid for OFDM systems in multipath environment. In this context, the transmitted signal components may be sent over the subcarriers simultaneously and are affected by independent fading by introducing a channel interleaver.

2.2 The Transmission System

Based on the above considerations about the channel model, we assume the communication system shown in Fig. 2.2.

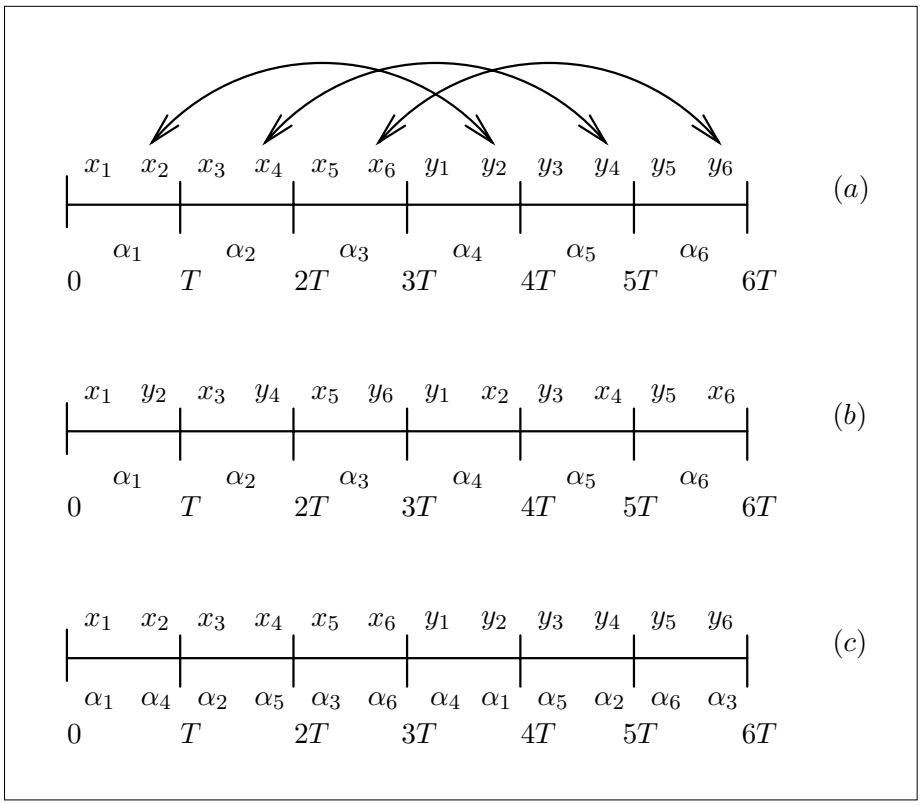

Fig. 2.1 The channel component interleaver/de-interleaver: (a) before interleaving at the transmitter, (b) on the channel, (c) after de-interleaving at the receiver

We consider n-dimensional signal constellations S carved from the set of lattice points $\{\mathbf{x} = \mathbf{u}M\}$, where $\mathbf{u}$ is an integer vector and M is the lattice generator matrix (see Section 3). The information bits may be used to label the integer components, as detailed in Section 2.4.

Let $\mathbf{x} = (x_1, x_2, \ldots x_n) \in \mathbb{R}^n$ denote a transmitted signal vector. Received signal samples are then given by $\mathbf{r} = (r_1, r_2, \ldots r_n)$ with $r_i = \alpha_i x_i + n_i$ for $i = 1, 2, \ldots n$, where the α_i are independent real Rayleigh random variables with unit second moment (i.e. $E[\alpha_i^2] = 1$) and n_i are real Gaussian random variables with mean zero and variance $N_0/2$ representing the additive noise. Using $*$ to represent the component-

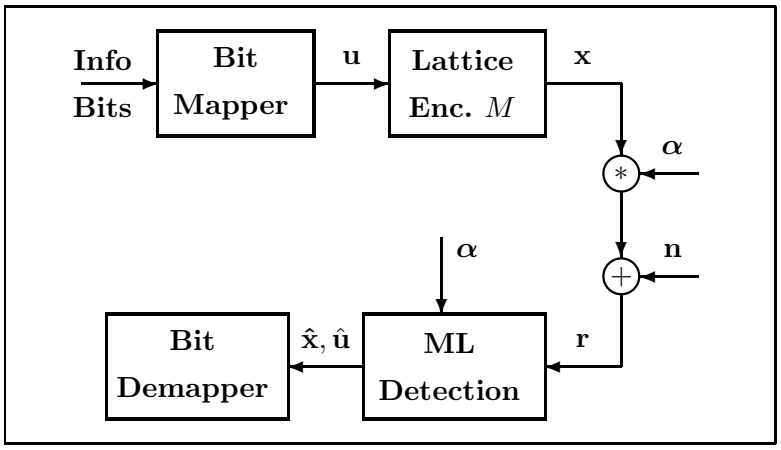

Fig. 2.2 Transmission system model

wise vector product, we can then write : $\mathbf{r} = \boldsymbol{\alpha} * \mathbf{x} + \mathbf{n}$, with $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots \alpha_n)$ and $\mathbf{n} = (n_1, n_2, \ldots n_n)$.

We assume that the receiver has knowledge of the fading coefficients, i.e., perfect channel state information (CSI). With perfect CSI, *Maximum Likelihood* (ML) detection requires the minimization of the following metric

$$m(\mathbf{x}|\mathbf{r}, \boldsymbol{\alpha}) = \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2. \tag{2.2}$$

We obtain the decoded point $\hat{\mathbf{x}}$ and the corresponding integer component vector $\hat{\mathbf{u}}$, from which the decoded bits can be extracted.

The minimization of (2.2) can be a very complex operation for an arbitrary signal set with a large number of points. It is shown in Section 4 how to apply a universal lattice decoder (*Sphere Decoder*) to obtain a more efficient ML detection of lattice constellations in fading channels. This is one of the most important reason for using lattice constellations.

2.3 Signal Space Diversity and Product Distance

In order to derive code design criteria, we estimate the codeword error probability $P_e(S)$ of the transmission system described in Section 2.2.

Since a lattice is *geometrically uniform* we may simply write $P_e(\Lambda) = P_e(\Lambda|\mathbf{0})$ for the point error probability. If we apply the union bound, we have the upper bound

$$P_e(S) \leq P_e(\Lambda) \leq \sum_{\mathbf{y} \neq \mathbf{x}} P(\mathbf{x} \to \mathbf{y}) \tag{2.3}$$

where $P(\mathbf{x} \to \mathbf{y})$ is the pairwise error probability. The first inequality takes into account the edge effects of the finite constellation S compared to the infinite lattice Λ.

Let us apply the standard Chernoff bound technique to estimate the pairwise error probability [12, 18]. For large signal to noise ratios we have

$$P(\mathbf{x} \to \mathbf{y}) \leq \frac{1}{2} \prod_{x_i \neq y_i} \frac{4N_0}{(x_i - y_i)^2} = \frac{1}{2} \frac{(4N_0)^l}{d_p^{(l)}(\mathbf{x}, \mathbf{y})^2} \tag{2.4}$$

where $d_p^{(l)}(\mathbf{x}, \mathbf{y})$ is the *l-product distance* of $\mathbf{x}$ from $\mathbf{y}$, when these two points differ in l components, i.e.,

$$d_p^{(l)}(\mathbf{x}, \mathbf{y}) = \prod_{x_i \neq y_i} |x_i - y_i|. \tag{2.5}$$

The asymptotically dominant terms in the sum in (2.3) are found for $L = \min(l)$, the *modulation diversity* or *diversity order* of the signal constellation. In other words, L is the minimum number of distinct components between any two constellation points or the minimum Hamming distance between any two coordinate vectors of the constellation points. Among the terms with the same diversity order, the dominant term is found for $d_{p,min} = \min d_p^{(L)}$.

> We conclude that the error probability is determined asymptotically by the diversity order L and the minimum product distance $d_{p,min}$. In particular, good signal sets have high L and $d_{p,min}$.

If the diversity order L equals the dimension of the lattice n, we say that the constellation has *maximal diversity*.

Finally, we note that the exact pairwise error probability $P(\mathbf{x} \to \mathbf{y})$ was computed in [47, 49, 48]. Although useful for a more accurate

performance evaluation, the complexity of the exact expression does not give a practical design criterion.

Example 2.1. Take a 4-QAM constellation. On Fig. 2.3(a), the diversity is $L = 1$, while on Fig. 2.3(b), a rotated version of the constellation (4-RQAM) has diversity $L = 2$, thus maximal diversity. Suppose now a fading of 0.5 affects the second component. In case (a), the points will get closer to each other and eventually collapse together if the fading is deeper. In this case, a very small amount of noise will produce a decoding error. In case (b), the rotated version, where all coordinates are distinct, will be more resistant to noise, even in the presence of a deep fade.

It is clear that any small rotation would be enough to obtain maximal diversity, but in order to optimize the choice, we must select the one that will give the lowest probability of error. This requires to consider the minimum product distance $d_{p,min}$. In this particular case, the optimal rotation which maximizes the $d_{p,min}$ is of 13 degrees.

In Fig. 2.4, we show the diversity gain of the rotated constellation with respect to the non-rotated one, as well as the error probability of the 4-QAM over the Gaussian channel. The gap between the curves represents the potential gain obtainable by increasing the diversity.

We will show that by increasing the diversity order of multidimensional constellations, it is possible to approach the performance of the transmission over Gaussian channel.

The first idea of rotating a two-dimensional signal constellation in order to gain diversity was shown in [9]. The attempt to find good rotations in higher dimensions by numerical optimization, without the aid of any algebraic structure, was only feasible up to four-dimensional constellations [36].

An interesting feature of the rotation operation is that the rotated signal set has exactly the same performance as the non-rotated one when used over a pure AWGN channel. As for other types of diversity such as space, time, frequency, and code diversity, the performance over Rayleigh fading channels, for increasingly high modulation diversity order, approaches that achievable over the Gaussian channel [54, 19].

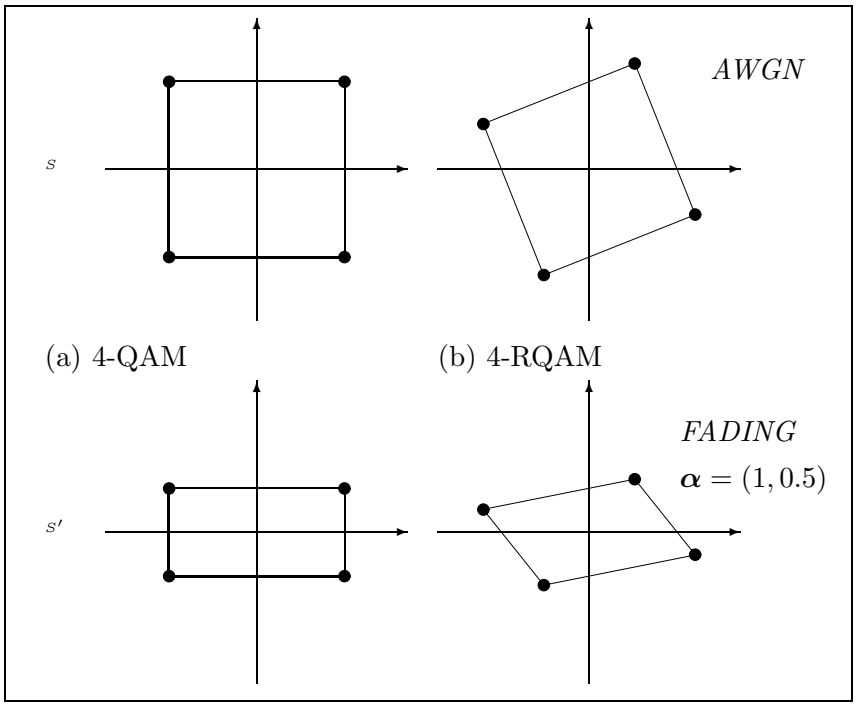

Fig. 2.3 Example of modulation diversity with 4-QAM: (a) $L = 1$, (b) $L = 2$.

2.4 Rotated $\mathbb{Z}^n$–lattice Constellations

In the design of the signal constellations, two fundamental operations should always be kept in mind: *bit labeling* and *constellation shaping*. These may be very critical for the complexity of practical implementations and are strictly related to each other. If we want to avoid the use of a huge look-up table to perform bit labeling, we need to have a simple algorithm mapping bits to signal points and vice-versa. On the other hand, it is well known that lattice constellations bounded by a sphere have the best shaping gain. Unfortunately, labeling a spherically shaped constellation is not always an easy task, without using a look-up table. Cubic shaped constellations offer a good trade-off: they are only slightly worse in terms of shaping gain but are usually easier to label.

The simplest labeling algorithm we can use for a lattice constel-

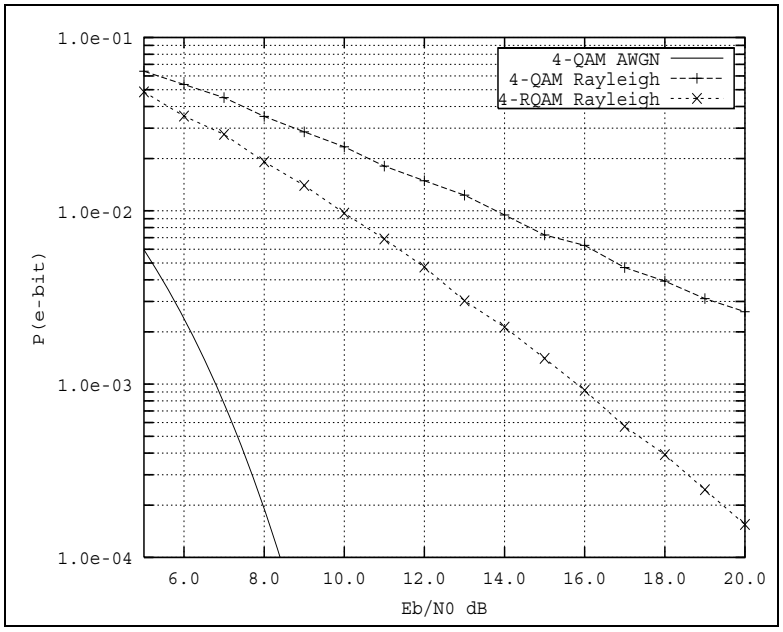

Fig. 2.4 Bit error probability of the 4-QAM and 4-RQAM over Gaussian and Rayleigh fading channels

lation $S = \{\mathbf{x} = \mathbf{u}M : \mathbf{u} = (u_1, \ldots, u_n) \in (q - \text{PAM})^n\}$ can be obtained by performing the bit labeling on the integer components u_i of the vector $\mathbf{u}$. These are usually restricted to a q-PAM constellation $\{\pm 1, \pm 3, \ldots, \pm(2^{\eta/2} - 1)\}$, where η is the number of bits per 2 dimension (or bit/symbol). Gray bit labeling of each q-PAM one dimensional component proved to be the most effective strategy to reduce the bit rate.

If we restrict ourselves to the above very simple labeling algorithm, we observe that this induces a constellation shape similar to the fundamental parallelotope (see Section 3) of the underlying lattice. This means that the constellation shape will not be cubic in general and hence will produce an undesirable shaping loss for all lattices except for $\mathbb{Z}^n$–lattices.

The option of using Voronoi constellations [28] was discarded for various reasons. First of all we note that the decoding requires non-marginal additional complexity in the lattice decoder to check for the

boundaries. Furthermore, the choice of a shaping sublattice which gives simple bit labeling does not necessarily lead to some shaping gains with algebraic lattices, since these are not particularly good sphere packings.

We conclude that a good compromise is to work with $\mathbb{Z}^n$–lattices, which may be found in their fully diverse rotated versions by the use of the algebraic constructions.

Finally, these signal constellations may be used either in a concatenated scheme with an outer code or in a coded modulation scheme using set partitioning [34, 29, 31, 30, 16, 14, 13].

3

Some Lattice Theory

In this section we review the very basic definitions of lattice theory, such as *fundamental parallelotope*, *Gram matrix*, *generator matrix* and *sublattice*. Our presentation follows [23], to which we let the reader refer for more details. Note that we will adopt the row vector convention.

3.1 First Definitions

We begin by recalling the definition of group, which will be useful both here, in the context of lattices, and later, in the section on algebraic number theory.

Definition 3.1. Let $\mathcal{G}$ be a set endowed with an internal operation (that we denote additively)

$$\begin{array}{ccc} \mathcal{G} \times \mathcal{G} & \to & \mathcal{G} \\ (a, b) & \mapsto & a + b \end{array}$$

The set $(\mathcal{G}, +)$ is a *group* if

(1) the operation is associative, i.e., $a + (b + c) = (a + b) + c$ for all $a, b, c \in \mathcal{G}$

(2) there exists a neutral element 0, such that $0 + a = a + 0$ for all $a \in \mathcal{G}$
(3) for all $a \in \mathcal{G}$, there exists an inverse $-a$ such that $a - a = -a + a = 0$.

The group $\mathcal{G}$ is said to be *Abelian* if $a + b = b + a$ for all $a, b \in \mathcal{G}$, i.e., the internal operation is commutative.

Definition 3.2. Let $(\mathcal{G}, +)$ be a group and $\mathcal{H}$ be a non-empty subset of $\mathcal{G}$. We say that $\mathcal{H}$ is a *subgroup* of $\mathcal{G}$ if $(\mathcal{H}, +)$ is a group, where $+$ is the internal operation inherited from $\mathcal{G}$.

An interesting point in having a group structure is that one is sure that whenever two elements are in the group, then their sum is also in the group. We say the group $\mathcal{G}$ is *closed* under the group operation $+$.

Definition 3.3. Let $\mathbf{v}_1, \ldots, \mathbf{v}_m$ be a linearly independent set of vectors in $\mathbb{R}^n$ (so that $m \leq n$). The set of points

$$\Lambda = \{\mathbf{x} = \sum_{i=1}^{m} \lambda_i \mathbf{v}_i,\ \lambda_i \in \mathbb{Z}\}$$

is called a *lattice* of dimension m, and $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ is called a *basis* of the lattice.

A lattice is a discrete set of points in $\mathbb{R}^n$. This is easily seen since we take integral linear combinations of $\mathbf{v}_1, \ldots, \mathbf{v}_m$. More precisely, it is a subgroup of $(\mathbb{R}^m, +)$, so that in particular the sum or difference of two vectors in the lattice are still in it. We say that a lattice of dimension m *spans* $\mathbb{R}^m \subseteq \mathbb{R}^n$ (recall that $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly independent in $\mathbb{R}^n$). See Fig. 3.1.

Definition 3.4. The parallelotope consisting of the points

$$\theta_1 \mathbf{v}_1 + \ldots + \theta_n \mathbf{v}_m, \quad 0 \leq \theta_i < 1$$

is called a *fundamental parallelotope* of the lattice (see Fig. 3.1).

A fundamental parallelotope is an example of a *fundamental region* for the lattice, that is, a building block which when repeated many times fills the whole space with just one lattice point in each copy.

There are many different ways of choosing a basis for a given lattice, as shown in Fig. 3.1, where the lattice represented by the points grid can have $\{\mathbf{v}, \mathbf{w}\}$ or $\{\mathbf{v}, \mathbf{w}'\}$ as a basis.

Let the coordinates of the basis vectors be

$$\begin{aligned} \mathbf{v}_1 &= (v_{11}, v_{12}, \ldots, v_{1n}), \\ \mathbf{v}_2 &= (v_{21}, v_{22}, \ldots, v_{2n}), \\ &\ldots \\ \mathbf{v}_m &= (v_{m1}, v_{m2}, \ldots, v_{mn}) \end{aligned}$$

where $n \geq m$.

Definition 3.5. The matrix

$$M = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ \ldots & & \ldots & \\ v_{m1} & v_{m2} & \ldots & v_{mn} \end{pmatrix}$$

is called a *generator matrix* for the lattice. The matrix $G = MM^T$ is called a *Gram matrix* for the lattice, where T denotes transposition.

More concisely, the lattice can be defined by its generator matrix as

$$\Lambda = \{\mathbf{x} = \boldsymbol{\lambda} M \mid \boldsymbol{\lambda} \in \mathbb{Z}^m\}.$$

Definition 3.6. The *determinant of the lattice* Λ is defined to be the determinant of the matrix G

$$\det(\Lambda) = \det(G).$$

This is an *invariant of the lattice*, since it does not depend on the choice of the lattice basis.

Since the Gram matrix is given by $G = MM^T$, where M contains the basis vectors $\{\mathbf{v}_i\}_{i=1}^m$ of the lattice, the (i, j)th entry of G is the inner product $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \mathbf{v}_i \cdot \mathbf{v}_j^T$.

Definition 3.7. A lattice Λ is called an *integral* lattice if its Gram matrix has coefficients in $\mathbb{Z}$.

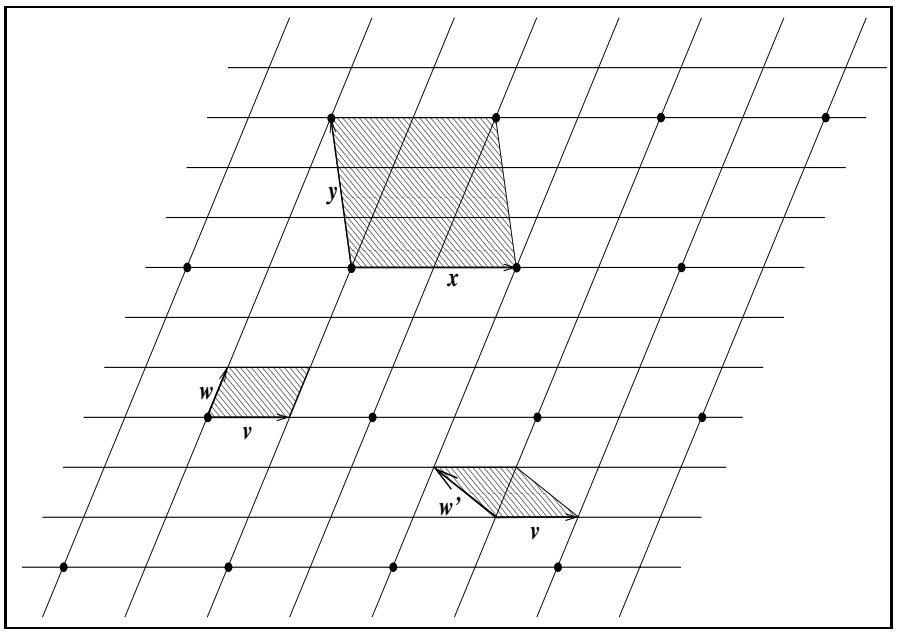

Fig. 3.1 The points grid represent a lattice. The set of vectors $\{\mathbf{v}, \mathbf{w}\}$ and $\{\mathbf{v}, \mathbf{w}'\}$ are two examples of basis for this lattice. They both span a fundamental parallelotope for the lattice. Points $\bullet$ represent a sublattice. The set of vectors $\{\mathbf{x}, \mathbf{y}\}$ form a basis for this sublattice. They span a fundamental parallelotope for the sublattice.

Remark 3.1. A lattice Λ is integral if and only if $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$, for all $\mathbf{x}, \mathbf{y} \in \Lambda$. Indeed, take $\mathbf{x}, \mathbf{y} \in \Lambda$, $\mathbf{x} = \sum_{i=1}^{m} \lambda_i \mathbf{v}_i$, $\mathbf{y} = \sum_{i=j}^{m} \mu_j \mathbf{v}_j$, with $\lambda_i, \mu_j \in \mathbb{Z}$. Thus $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i,j=1}^{n} \lambda_i \mu_j v_i v_j^T = \sum_{i,j=1}^{n} \lambda_i \mu_j g_{ij}$. If Λ is integral, $g_{ij} \in \mathbb{Z}$ for all i, j, and $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$. The other implication is immediate.

In all the rest of this work we will deal with *full-rank* lattices i.e., $m = n$. In this case, M is a square matrix and we have

$$\det(\Lambda) = (\det(M))^2.$$

Definition 3.8. For full-rank lattices, the square root of the determinant is the volume of the fundamental parallelotope, also called *volume of the lattice*, and denoted by $vol(\Lambda)$.

3.2 Sublattices and Equivalent Lattices

Let Λ be a lattice of dimension n defined by its generator matrix M.

Definition 3.9. Let B be an $n \times n$ integer matrix. A *sublattice* of Λ is given by

$$\Lambda' = \{\mathbf{x} = \boldsymbol{\lambda} BM \mid \boldsymbol{\lambda} \in \mathbb{Z}^n\}.$$

Since a lattice has a group structure, a sublattice Λ' is then a subgroup of Λ, and as such, we may consider the *quotient group* Λ/Λ'. For convenience, we recall how to define a quotient group.

Definition 3.10. Let G be a group (written additively), and H be a subgroup of G. Let $a \in G$. The subset

$$a + H = \{a + h,\ h \in H\} \text{ (resp. } H + a = \{h + a,\ h \in H\})$$

is called a left (resp. right) *coset* of G modulo H.

If G is Abelian, then the distinction between left and right cosets modulo H is unnecessary. It can be shown ([37, p. 6]) that a group G can be partitioned into cosets modulo H. For our purposes, we restrict the following definition to Abelian groups.

Definition 3.11. For a subgroup H of an Abelian group G, the group formed by the cosets of G modulo H under the operation $(a + H) + (b + H) = (a + b)H$ is called the *quotient group* of G modulo H, and denoted by G/H.

We let the reader refer to [37, p. 9] for more details, and the proof that the structure described in the definition is actually a group. Let us now return to the quotient of a lattice Λ by one of its sublattices Λ' (see Fig. 3.2).

Definition 3.12. The *index of the sublattice* $\Lambda' = \{\mathbf{x} = \boldsymbol{\lambda} BM \mid \boldsymbol{\lambda} \in \mathbb{Z}^n\}$ is the cardinality of the quotient group Λ/Λ' and we have [43]:

$$|\Lambda/\Lambda'| = \frac{vol(\Lambda')}{vol(\Lambda)} = |\det(B)|.$$

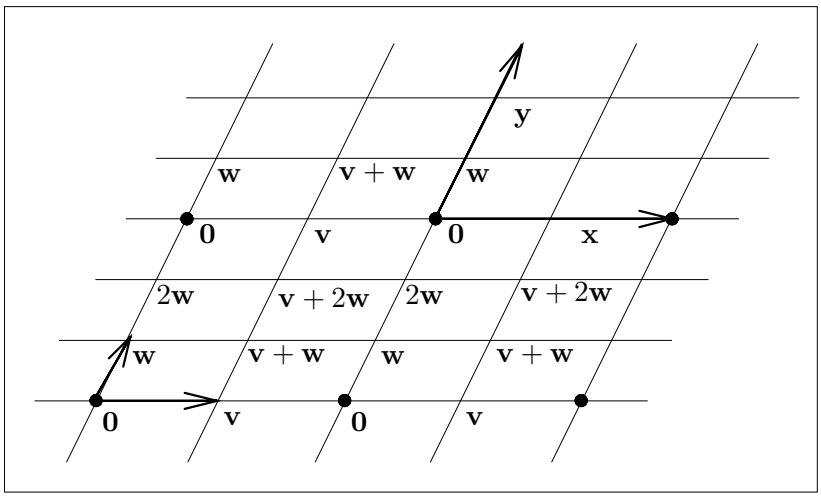

Fig. 3.2 A way of visualizing the quotient group Λ/Λ': the grid represents a lattice Λ with basis $\{\mathbf{v}, \mathbf{w}\}$, and the $\bullet$ represent a sublattice Λ' with basis $\{\mathbf{x}, \mathbf{y}\}$. Points in Λ' are identified to zero in the quotient group Λ/Λ'.

Example 3.1. Consider the lattice Λ and its sublattice Λ' given in Fig. 3.2, whose bases are $\{\mathbf{v}, \mathbf{w}\}$ resp. $\{\mathbf{x}, \mathbf{y}\}$. We have

$$\begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} = B \begin{pmatrix} \mathbf{v} \\ \mathbf{w} \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} \mathbf{v} \\ \mathbf{w} \end{pmatrix}.$$

The determinant of B is 6. It is the cardinality of the quotient group whose elements can be written as $\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$. The group operation is a component-wise addition modulo 2 and modulo 3, respectively.

It is always possible to find a sublattice of a given lattice considering its *scaled version* by an integer factor.

Definition 3.13. Given a lattice Λ, a *scaled lattice* Λ' can be obtained multiplying all the vectors of the lattice by a constant:

$$\Lambda' = c \cdot \Lambda$$

where $c \in \mathbb{R}$. Thus Λ' is a sublattice of Λ when $c \in \mathbb{Z}$.

More generally, we have the following definition.

Definition 3.14. If one lattice can be obtained from another by (possibly) a rotation, reflection and change of scale, we say that they are *equivalent*.

Consequently, two generator matrices M and M' define equivalent lattices if and only if they are related by $M' = cUMB$, where c is a nonzero constant, U is a matrix with integer entries and determinant ± 1 (*unimodular integer matrix*), and B is a real orthogonal matrix (with $BB^T = I_n$). The corresponding Gram matrices are related by $G' = c^2 UGU^T$.

Thus one has to keep in mind that the same lattice may be represented in several different ways. As a consequence, given a Gram (or generator) matrix, it is not easy to determine which is the corresponding lattice. Invariants such as the dimension and the determinant will help, but one has to be careful that having the same determinant is not a sufficient condition for two lattices to be equivalent. These considerations will be of importance later, when we will build algebraic lattice constellations where the particular orientation of the lattice within the Euclidean space becomes important.

3.3 Two Famous Lattices

To conclude this section on lattice theory, we give two examples of famous lattices.

• **Integer lattices** $\mathbb{Z}^n$

These are the simplest lattices we can think of. For $n = 2$, this is a square grid (see Fig. 3.3). Formally we can write

$$\mathbb{Z}^n = \{(x_1, \ldots, x_n),\ x_i \in \mathbb{Z}\}.$$

Both the generator and the Gram matrices are the identity matrix.

• **Lattices** A_n

This lattice is well-known in dimension 2, where A_2 is called the *hexagonal lattice* (see Fig. 3.4). In general, it has a simple definition in

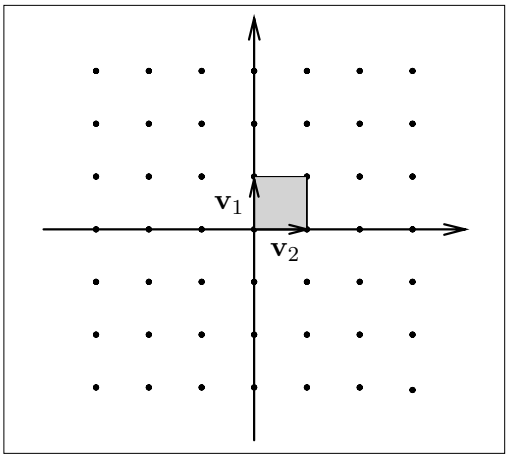

Fig. 3.3 The lattice $\mathbb{Z}^2$: a basis is given by $\{\mathbf{v}_1, \mathbf{v}_2\}$. The volume of the fundamental parallelotope is 1.

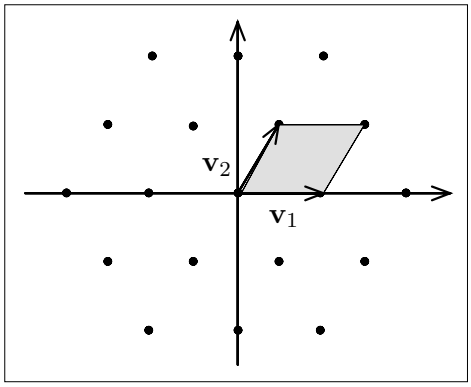

Fig. 3.4 The lattice A_2: a basis is given by $\{\mathbf{v}_1, \mathbf{v}_2\}$. The volume of the fundamental parallelotope is $\sqrt{3}$.

the $(n+1)$-dimensional space as

$$A_n = \{(x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1}, \ \sum_{i=0}^{n} x_i = 0\}.$$

Its Gram matrix is

$$G = \begin{pmatrix} 2 & -1 & 0 & \dots & 0 \\ -1 & 2 & -1 & & 0 \\ 0 & -1 & 2 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 2 \end{pmatrix}$$

3.4 Lattice Packings and Coverings

A very old problem in mathematics asks to stack a large number of identical 3-dimensional spheres in a very large box in the most efficient way, i.e., by maximizing the number of spheres which can fit inside the box. Such arrangements of spheres are called *sphere packings*. The spheres will not fill all the space in the box and whatever arrangement is chosen at least about 25% of the space remains empty. We call *packing density* Δ the percentage of space occupied by the spheres.

The above problem can be generalized to higher or lower dimensions, but the optimal or *densest* sphere packing is only known in dimensions 1 and 2 (Fig. 3.5). In all other dimensions we only have some good candidates.

Among all possible packings of spheres we distinguish the *lattice sphere packings* which are obtained by centering at each point of a full-rank lattice Λ, identical spheres with the maximum radius such that they do non penetrate into each other. This particular radius ρ is called *packing radius* of Λ. If we restrict the problem to lattice sphere packings, we know the optimal lattice sphere packing up to dimension 8.

The *covering problem* asks for the most economical way to cover the entire space with equal overlapping spheres (Fig. 3.6). Here, we only discuss lattice coverings, for which the centers of the spheres form a lattice. Given a full-rank lattice in $\mathbb{R}^n$, we call *covering radius* R of Λ the smallest radius for which the spheres still cover the entire space. R is also the distance of the furthest point of $\mathbb{R}^n$ from any lattice point.

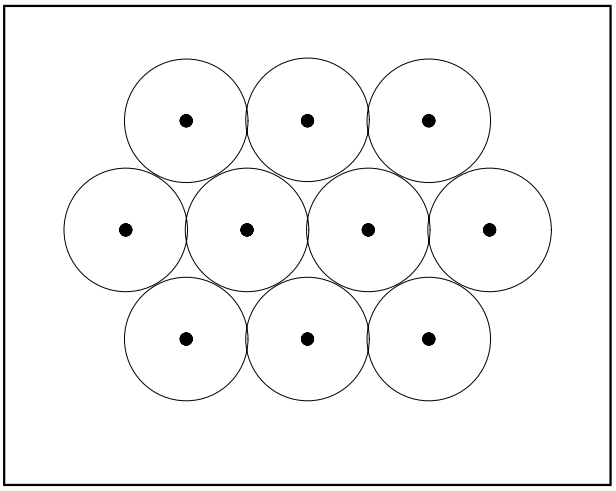

Fig. 3.5 The optimal 2-dimensional lattice sphere packing.

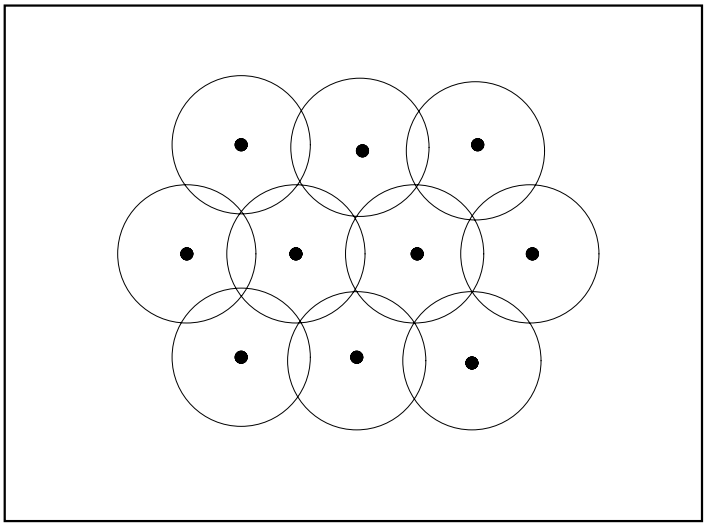

Fig. 3.6 The optimal 2-dimensional lattice covering.

4

The Sphere Decoder: A Universal Lattice Decoding Algorithm

The Sphere Decoder is a ML decoder for arbitrary lattice constellations. It solves the *closest lattice point problem*, i.e., it finds the closest lattice point to a given received point. At the basis of the Sphere Decoder is the Finke–Pohst algorithm which enumerates all lattice points within a sphere centered at the origin [27]. With minor adaptations it is possible to obtain an efficient lattice decoder. Recent work [26] has shown that the Sphere Decoder can be formulated as a stack algorithm and shows its relation to other well-known detection algorithms. In this section we focus on the purely geometric interpretation of this algorithm.

The key idea which makes the Sphere Decoder efficient is that the number of lattice points which are found inside a sphere is significantly smaller than the number of points within a hypercube containing the hypersphere as the dimension of the space grows.

To avoid the exhaustive enumeration of all points of the constellation, the lattice decoding algorithm searches through the points of the lattice Λ which are found inside a sphere of given radius $\sqrt{C}$ centered at the received point as shown in Fig. 4.1. This guarantees that only the lattice points within the squared distance C from the received point are considered in the metric minimization.

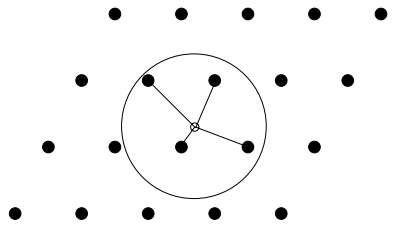

Fig. 4.1 Sphere of radius $\sqrt{C}$ centered at the received point.

The key steps of this algorithm are:

(1) Set the origin at the received point $\mathbf{r}$.
(2) Consider the lattice $\Lambda = \{\mathbf{x} = \mathbf{u}M | \mathbf{u} \in \mathbb{Z}^n\}$.
(3) Define the function $Q(\mathbf{u}) = ||\mathbf{x}||^2 = \mathbf{x}\mathbf{x}^T = \mathbf{u}G\mathbf{u}^T$, where $G = MM^T$ is the Gram matrix.
(4) Find all points in the sphere of square radius C by solving the inequality $Q(\mathbf{u}) \leq C$.
(5) Choose $\mathbf{x}$ minimizing $||\mathbf{r} - \mathbf{x}||^2$.

In order to perform ML decoding on high diversity lattice constellations with fading, some further modifications are required. In fact, for a given fading vector $\boldsymbol{\alpha}$, we need to decode a lattice with generator matrix $M\text{diag}(\boldsymbol{\alpha})$.

4.1 The Sphere Decoder Algorithm

The closest lattice point algorithm was first presented in [41] and further analyzed in [27]. In [51] the explicit geometric interpretation in terms of Sphere Decoder was shown.

In the following, it will be useful to think of the lattice Λ as the result of a linear transformation, defined by the matrix $M : \mathbb{R}^n \to \mathbb{R}^n$, when applied to the $\mathbb{Z}^n$–lattice. So Λ can be seen as a skewed version of the $\mathbb{Z}^n$–lattice.

The problem to solve is the following:

$$\min_{\mathbf{x}\in\Lambda} \|\mathbf{r} - \mathbf{x}\|^2 = \min_{\mathbf{w}\in\mathbf{r}-\Lambda} \|\mathbf{w}\|^2 \ . \tag{4.1}$$

that is, we search for the shortest vector $\mathbf{w}$ in the translated lattice $\mathbf{r} - \Lambda$ in the n-dimensional Euclidean space $\mathbb{R}^n$.

We write $\mathbf{x} = \mathbf{u}M$ with $\mathbf{u} \in \mathbb{Z}^n$, $\mathbf{r} = \boldsymbol{\rho}M$ with $\boldsymbol{\rho} = (\rho_1, \ldots, \rho_n) \in \mathbb{R}^n$, and $\mathbf{w} = \boldsymbol{\xi}M$ with $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_n) \in \mathbb{R}^n$.

Note that we have $\mathbf{w} = \sum_{i=1}^{n} \xi_i \mathbf{v}_i$, where the $\mathbf{v}_i$ are the lattice basis vectors and the $\xi_i = \rho_i - u_i,\ i = 1, \ldots, n$ define the translated coordinate axes in the space of the integer component vectors $\mathbf{u}$ of the $\mathbb{Z}^n$–lattice.

The sphere of square radius C, centered at the received point, is transformed into an ellipsoid centered at the origin of the new coordinate system defined by $\boldsymbol{\xi}$:

$$\|\mathbf{w}\|^2 = Q(\boldsymbol{\xi}) = \boldsymbol{\xi}MM^T\boldsymbol{\xi}^T = \boldsymbol{\xi}G\boldsymbol{\xi}^T = \sum_{i=1}^{n}\sum_{j=1}^{n} g_{ij}\xi_i\xi_j \leq C\ . \qquad (4.2)$$

Cholesky's factorization of the Gram matrix $G = MM^T$ yields $G = R^TR$, where R is an upper triangular matrix. Then

$$Q(\boldsymbol{\xi}) = \boldsymbol{\xi}R^TR\boldsymbol{\xi}^T = \|R\boldsymbol{\xi}^T\|^2 = \sum_{i=1}^{n}\left(r_{ii}\xi_i + \sum_{j=i+1}^{n} r_{ij}\xi_j\right)^2 \leq C\ . \quad (4.3)$$

Substituting $q_{ii} = r_{ii}^2$ for $i = 1, \ldots, n$ and $q_{ij} = r_{ij}/r_{ii}$ for $i = 1, \ldots n$, $j = i+1, \ldots, n$, we can write

$$Q(\boldsymbol{\xi}) = \sum_{i=1}^{n} q_{ii}\left(\xi_i + \sum_{j=i+1}^{n} q_{ij}\xi_j\right)^2 = \sum_{i=1}^{n} q_{ii}U_i^2 \leq C\ , \qquad (4.4)$$

where the new coordinate system defined by the

$$U_i = \xi_i + \sum_{j=i+1}^{n} q_{ij}\xi_j, \qquad i = 1, \ldots n \qquad (4.5)$$

defines an ellipsoid in its canonical form. Starting from U_n and working backwards, we find the equations of the border of the ellipsoid as

$$\begin{aligned} -\sqrt{\frac{C}{q_{nn}}} \leq \quad & U_n \quad \leq \sqrt{\frac{C}{q_{nn}}} \\ -\sqrt{\frac{C - q_{nn}U_n}{q_{n-1,n-1}}} \leq \quad & U_{n-1} \quad \leq \sqrt{\frac{C - q_{nn}U_n}{q_{n-1,n-1}}} \\ & \vdots \end{aligned} \qquad (4.6)$$

The corresponding ranges for the integer components u_n and u_{n-1} are found by replacing $\xi_i = \rho_i - u_i$ in (4.5) and (4.6)

$$\left\lceil -\sqrt{\frac{C}{q_{nn}}} + \rho_n \right\rceil \leq u_n \leq \left\lfloor \sqrt{\frac{C}{q_{nn}}} + \rho_n \right\rfloor$$

$$\begin{aligned} \left\lceil -\sqrt{\frac{C - q_{nn}\xi_n^2}{q_{n-1,n-1}}} + \rho_{n-1} + q_{n-1,n}\xi_n \right\rceil &\leq u_{n-1} \\ \leq \left\lfloor \sqrt{\frac{C - q_{nn}\xi_n^2}{q_{n-1,n-1}}} + \rho_{n-1} + q_{n-1,n}\xi_n \right\rfloor & \end{aligned}$$

where $\lceil x \rceil$ is the smallest integer greater than x and $\lfloor x \rfloor$ is the greatest integer smaller than x. For the i-th integer component we have

$$\begin{aligned} \left\lceil -\sqrt{\frac{1}{q_{ii}}\left(C - \sum_{l=i+1}^{n} q_{ll}\left(\xi_l + \sum_{j=l+1}^{n} q_{lj}\xi_j\right)^2\right)} + \rho_i + \sum_{j=i+1}^{n} q_{ij}\xi_j \right\rceil & \\ \leq u_i & \\ \leq \left\lfloor \sqrt{\frac{1}{q_{ii}}\left(C - \sum_{l=i+1}^{n} q_{ll}\left(\xi_l + \sum_{j=l+1}^{n} q_{lj}\xi_j\right)^2\right)} + \rho_i + \sum_{j=i+1}^{n} q_{ij}\xi_j \right\rfloor & \end{aligned} \tag{4.7}$$

To gain a simple geometric insight, we set the origin of the coordinate system in $\mathbf{r} = \mathbf{0}$ (i.e., $\rho_i = 0, i = 1, \ldots, n$), so that the Sphere Decoder reduces to the Finke–Pohst enumeration algorithm. The three basic steps of the algorithm are illustrated in Figures 4.2, 4.3 and 4.4, which give the geometric interpretation of the operations involved in the Sphere Decoder.

(1) The sphere is centered at the origin and includes the lattice points to be enumerated, Fig. 4.2.
(2) The sphere is transformed into an ellipsoid in the integer lattice domain, Fig. 4.3.
(3) The rotation into the new coordinate system defined by the U_i's enables to enumerate the $\mathbb{Z}^n$–lattice points. The points

inside the ellipse in Fig. 4.4 are visited from the bottom to the top and from left to right.

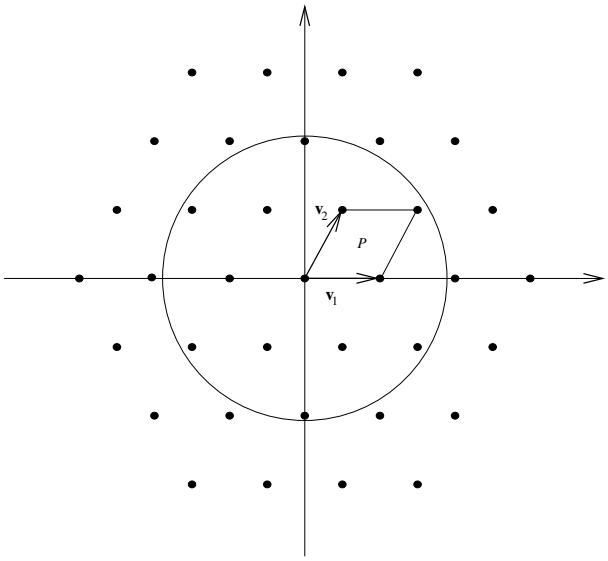

Fig. 4.2 The sphere is centered at the origin and includes the lattice points to be enumerated.

The search algorithm proceeds very much like a mixed radix counter on the digits u_i, with the addition that the bounds change whenever there is a carry operation from one digit to the next. In practice, the bounds can be updated recursively by using the following equations

$$\begin{aligned} S_i = S_i(\xi_{i+1}, \ldots, \xi_n) &= \rho_i + \sum_{l=i+1}^{n} q_{il}\xi_l \\ T_{i-1} = T_{i-1}(\xi_i, \ldots, \xi_n) &= C - \sum_{l=i}^{n} q_{ll} \left(\xi_l + \sum_{j=l+1}^{n} q_{lj}\xi_j \right)^2 \\ &= T_i - q_{ii}\,(S_i - u_i)^2 \end{aligned}$$

When a vector inside the sphere is found, its square distance from the center (the received point) is given by

$$\hat{d}^2 = C - T_1 + q_{11}(S_1 - u_1)^2 \ .$$

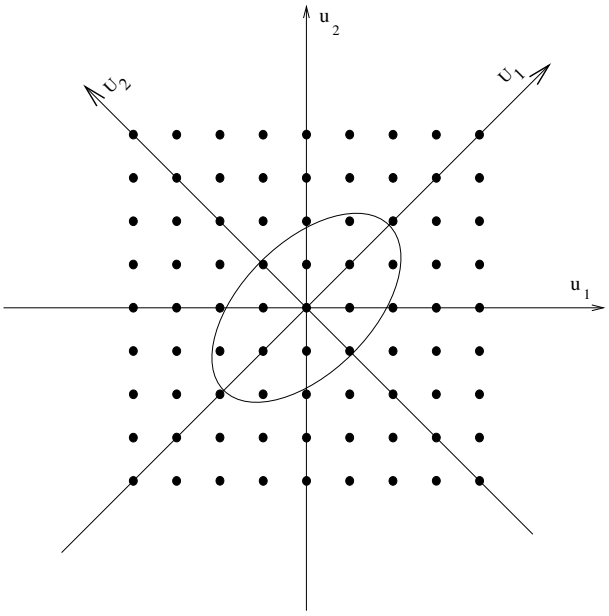

Fig. 4.3 The sphere is transformed into an ellipsoid in the integer lattice domain.

This value is compared to the minimum square distance d^2 (initially set equal to C) found so far in the search. If it is smaller then we have a new candidate closest point and the search can go on using a new sphere with smaller radius.

The advantage of this method is that we never test vectors with a norm greater than the given radius. Every tested vector requires the computation of its norm, which entails n multiplications and $n-1$ additions. The increase in the number of operations needed to update the bounds (4.7) is largely compensated for by the enormous reduction in the number of vectors tested especially when the dimension increases.

In order to be sure to always find a lattice point inside the sphere we must select $\sqrt{C}$ equal to the covering radius of the lattice. Otherwise, we do *bounded distance decoding* and the decoder can signal an erasure whenever no point is found inside the sphere. A judicious choice of C can greatly speed up the decoder. In practice the choice of C can be adjusted according to the noise variance N_0 so that the probability of

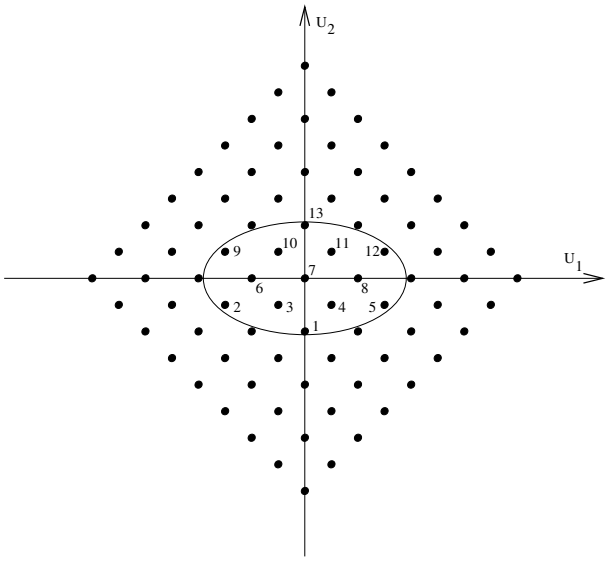

Fig. 4.4 The coordinate rotation enables to enumerate the $\mathbb{Z}^n$–lattice points.

a decoding failure is negligible. If a decoding failure is detected, the operation can either be repeated with a greater radius or an erasure can be declared.

The kernel of the Sphere Decoder (the enumeration of lattice points inside a sphere of radius $\sqrt{C}$) requires the greatest number of operations. The complexity is obviously independent of the constellation size, i.e. the number of operations does not depend on the spectral efficiency of the signal constellation.

The complexity analysis presented in [27] shows that if d^{-1} is a lower bound for the eigenvalues of the Gram matrix G, then the number of arithmetical operations is

$$O\left(n^2 \times \left(1 + \frac{n-1}{4dC}\right)^{4dC}\right) . \tag{4.8}$$

For a fixed radius and a given lattice (which fixes d), the complexity of the decoding algorithm is polynomial. We would like to notice that this does not mean that the general lattice decoding problem is not NP-hard. In fact, it is possible to construct a sequence of lattices of

increasing dimension with an increasing value of the exponent d.

The above complexity estimate is very pessimistic, since it does not take into account the fact that we are dealing with an AWGN channel. In such a case, it was shown in [35] that for a wide range of signal-to-noise ratios and dimensions the expected complexity is essentially polynomial as $O(n^3)$.

When we deal with a lattice constellation, we must consider the edge effects. During the search in the sphere, we discard the points which do not belong to the lattice code; if no code vector is found we declare an erasure. The complexity of this additional test depends on the shape of the constellation.

For cubic shaped constellations, it only entails checking that the vector components lie within a given range. For a spherically shaped signal set, it is sufficient to compute the length of the code vector found in the search sphere in order to check if it is within the outermost shell of the constellation.

4.2 The Sphere Decoder with Fading

For ML decoding with perfect CSI at the receiver, the problem is to minimize the metric (2.2). Let M be the generator matrix of the lattice Λ and let us consider the lattice Λ_c with generator matrix

$$M_c = M \,\mathrm{diag}(\alpha_1, \dots \alpha_n) \ .$$

We can imagine this new lattice Λ_c in a space where each component has been compressed or enlarged by a factor α_i. A point of Λ_c can be written as $\mathbf{x}^{(c)} = (x_1^{(c)}, \dots x_n^{(c)}) = (\alpha_1 x_1, \dots \alpha_n x_n)$. The metric to minimize is then

$$m(\mathbf{x}|\mathbf{r}, \boldsymbol{\alpha}) = \sum_{i=1}^{n} |r_i - x_i^{(c)}|^2 \ .$$

This means that we can simply apply the lattice decoding algorithm to the lattice Λ_c, when the received point is $\mathbf{r}$. The decoded point $\hat{\mathbf{x}}^{(c)} \in \Lambda_c$ has the same integer components $(\hat{u_1}, \dots \hat{u_n})$ as $\hat{\mathbf{x}} \in \Lambda$.

The additional complexity required by this decoding algorithm comes from the fact that for each received point we have a different

compressed lattice Λ_c. So we need to compute a new Cholesky factorization of the Gram matrix for each Λ_c, which requires $O(n^3/3)$ operations. We also need $M_c^{-1} = \mathrm{diag}(1/\alpha_1, \ldots 1/\alpha_n)M^{-1}$ to find the ρ_i's, but this only requires a vector-matrix multiplication since M^{-1} is precomputed. The complete flow-chart of the algorithm is given in Figure 4.5.

The choice of C in this case is more critical. In fact whenever we are in the presence of deep fades, then many points fall inside the search sphere and the decoding can be very slow. This is also evident from the fact that the Gram matrix of Λ_c may have a very small eigenvalue which gives a large exponent d in (4.8). This problem may be partially overcome by adapting C according to the values of the fading coefficients α_i. A good choice for C was found to be the smallest element of the diagonal of the Gram matrix of Λ_c. Note that the elements on the diagonal of the Gram matrix are the squared lengths of the basis vectors. A lattice base reduction may be useful to reduce the search radius but requires additional overhead (see [1]).

4.3 Conclusions

Decoding arbitrary signal constellations in a fading environment can be a very complex task. When the signal set has no structure it is only possible to perform an exhaustive search through all the constellation points. Some signal constellations, which can be efficiently decoded when used over the Gaussian channel, become hard to decode when used over the fading channel since their structure is destroyed. Fortunately, for lattice constellations this is not the case since the faded constellation still preserves a lattice structure and only a small additional complexity is required.

The interest in lattice decoding has steadily grown in the last few years. This algorithm was also successfully applied to ML decoding of MIMO and DS-CDMA systems [25, 20]. An interesting alternative to the Sphere Decoding is given by the Shnorr–Euchner strategy presented in [1].

Further optimization of the decoding strategy based on the appro-

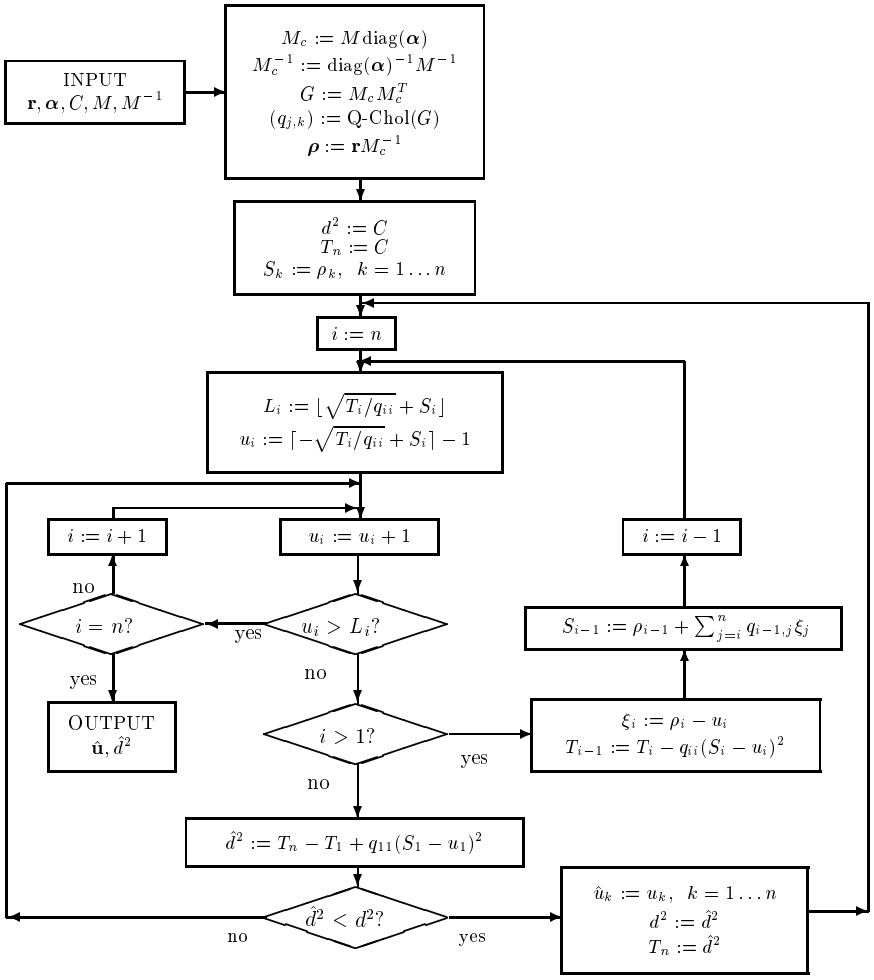

Fig. 4.5 Flow chart of the Sphere Decoder

priate choice of the initial radius is still under investigation. This depends on the specific application and may marginally extend the range of feasible dimensions, currently around $n = 32$. In order to increase significantly the dimensions, suboptimal (near-ML) strategies should be considered. We address the reader to [26] to see how the Sphere Decoder can be formulated as a stack algorithm, which enables the for-

mulation of a large variety of decoding strategies ranging from ML to the Fano sequential decoder. A rich area of research is still open concerning the practical implementation of lattice decoding algorithms.

5

First Concepts in Algebraic Number Theory

In this section, we introduce some elementary concepts of algebraic number theory. We will present only the relevant definitions and results which lead to algebraic lattice constructions. The exposition is self-contained and is based on simple examples. Precise references are given, so that the interested reader may easily fill in the proofs and the missing details. Some elementary books on number theory are given in the bibliography (e.g. [43, 45, 22]).

Algebraic number theory is roughly speaking the study of numbers. Typical questions that arise are related to the factorization of numbers, or to the solutions of algebraic equations. Due to its historical importance, Fermat's Last Theorem is probably the most famous example of a problem that came from algebraic number theory. Recall that the question was to prove that the equation

$$x^n + y^n = z^n \quad x, y, z \in \mathbb{Z}$$

has no non-trivial solution if $n \geq 3$. Trying to solve such problems led mathematicians to introduce new objects and build new theories, some of them being now part of the "common" background of number theory. Far from all this, the scope of this section is, starting from the

familiar sets $\mathbb{Z}$ and $\mathbb{Q}$, to define concepts such as

- a number field K, its ring of integers $\mathcal{O}_K$ and its integral basis
- invariants of a number field: discriminant and signature
- the embeddings of a number field into $\mathbb{C}$
- algebraic lattices, or how to build a lattice from a number field

5.1 Algebraic Number Fields

Let $\mathbb{Z}$ be the set of rational integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ and let $\mathbb{Q}$ be the set of rational numbers $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$. Starting from these two sets, the goal of this first section is to define algebraic structures so as to end up with the notion of *number field*.

Definition 5.1. Let A be a set endowed with two internal operations denoted by $+$ and $\cdot$

$$\begin{array}{ccc} A \times A & \to & A \\ (a,b) & \mapsto & a+b \end{array} \quad \text{and} \quad \begin{array}{ccc} A \times A & \to & A \\ (a,b) & \mapsto & a \cdot b \end{array}$$

The set $(A, +, \cdot)$ is a *ring* if

(1) $(A, +)$ is an Abelian group (Definition 3.1)
(2) the operation $\cdot$ is associative, i.e., $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in A$ and has a neutral element 1 such that $1 \cdot a = a \cdot 1$ for all $a \in A$
(3) the operation $\cdot$ is distributive over $+$, i.e., $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(a+b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in A$.

The ring A is *commutative* if $a \cdot b = b \cdot a$ for all $a, b \in A$. The set of elements of A that are invertible for the operation $\cdot$ is called the set of *units* of A, and is denoted by A^*.

The set $\mathbb{Z}$ is easily checked to be a ring. Its units are $\mathbb{Z}^* = \{1, -1\}$.

Definition 5.2. Let A be a ring such that $A^* = A \backslash \{0\}$. Then A is said to be a *skew field*. If A is moreover commutative, it is said to be a *field*.

The set $\mathbb{Q}$ is easily checked to be a field. Other examples of fields can be built starting from $\mathbb{Q}$. Take for example $\sqrt{2}$, which is not an element of $\mathbb{Q}$. One can build a new field "adding" $\sqrt{2}$ to $\mathbb{Q}$. Note that in order to make this new set a field, we have to add all the multiples and all the powers of $\sqrt{2}$. We thus get a new field that contains both $\mathbb{Q}$ and $\sqrt{2}$, that we denote by $\mathbb{Q}(\sqrt{2})$. We call it a field extension of $\mathbb{Q}$. Let us formalize this procedure.

Definition 5.3. Let K and L be two fields. If $K \subseteq L$, we say that L is a *field extension* of K. We denote it L/K.

It is useful to note that if L/K is a field extension, then L has a natural structure of a vector space over K, where vector addition is addition in L and scalar multiplication of $a \in K$ on $v \in L$ is just $av \in L$. For example, an element $x \in \mathbb{Q}(\sqrt{2})$ can be written as $x = a + b\sqrt{2}$, where $\{1, \sqrt{2}\}$ are the basis "vectors" and $a, b \in \mathbb{Q}$ are the scalars. The dimension of $\mathbb{Q}(\sqrt{2})$ considered as vector space over $\mathbb{Q}$ is 2.

Definition 5.4. Let L/K be a field extension. The dimension of L as vector space over K is called the *degree* of L over K and is denoted by $[L : K]$. If $[L : K]$ is finite, we say that L is a *finite extension* of K.

A particular case of finite extension will be of great importance for us.

Definition 5.5. A finite extension of $\mathbb{Q}$ is called a *number field*.

Going on with our previous example, observe that a way to describe $\sqrt{2}$ is to say that this number is the solution of the equation $X^2 - 2 = 0$. Building $\mathbb{Q}(\sqrt{2})$, we thus add to $\mathbb{Q}$ the solution of a polynomial equation with integers coefficients. The number $\sqrt{2}$ is said to be algebraic.

Definition 5.6. Let L/K be a field extension, and let $\alpha \in L$. If there exists a non-zero irreducible monic (with highest coefficient 1) polynomial $p \in K[X]$ such that $p(\alpha) = 0$, we say that α is *algebraic* over K. Such a polynomial is called the *minimal polynomial* of α over K. We denote it by p_α.

In our example, the polynomial $X^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$.

Definition 5.7. If all the elements of K are algebraic, we say that K is an *algebraic extension* of $\mathbb{Q}$.

Consider the field $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2},\ \ a, b \in \mathbb{Q}\}$. It is simple to see that any $\alpha \in \mathbb{Q}(\sqrt{2})$ is a root of the polynomial $p_\alpha(X) = X^2 - 2aX + a^2 - 2b^2$ with rational coefficients. We conclude that $\mathbb{Q}(\sqrt{2})$ is an algebraic extension of $\mathbb{Q}$.

Remark 5.1. Since it can be shown that a finite extension is an algebraic extension (see [45, p. 23]), we also call equivalently a number field (Definition 5.5) an *algebraic number field*.

Now that we have set up the framework, we will concentrate on the particular fields that are number fields, that is field extensions $K/\mathbb{Q}$, with $[K : \mathbb{Q}]$ finite. Algebraic elements over $\mathbb{Q}$ are simply called algebraic numbers. In the following, K will denote a number field.

Theorem 5.1. [45, p. 40] If K is a number field, then $K = \mathbb{Q}(\theta)$ for some algebraic number $\theta \in K$, called *primitive element*.

As a consequence, K is a $\mathbb{Q}$–vector space generated by the powers of θ. If K has degree n then $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a *basis* of K and the degree of the minimal polynomial of θ is n.

Remark 5.2. Computations in $K = \mathbb{Q}(\theta)$, a number field of degree n as above, are done as follows. Let $p_\theta(X) = \sum_{i=0}^{n} p_i X^i$, $p_i \in \mathbb{Q}$ for all i, $p_n = 1$, denote the minimal polynomial of θ. Since $p_\theta(\theta) = 0$, this yields an equation of degree n in θ:

$$\theta^n = -\sum_{i=0}^{n-1} p_i \theta^i.$$

Likewise, θ^{n+j} is given by

$$\theta^{n+j} = -\sum_{i=0}^{n-1} p_i \theta^{i+j},\ \ j \geq 1,$$

where each θ^{i+j} with $i + j \geq n$ can be reduced recursively so as to obtain an expression in the basis $\{1, \theta, \ldots, \theta^{n-1}\}$.

A similar way of looking at these computations is to represent an element $a = \sum_{i=0}^{n-1} a_i \theta^i \in K$ as a polynomial $a(X) = \sum_{i=0}^{n-1} a_i X^i$. Operations between two elements $a, b \in K$ are performed on the two corresponding polynomials $a(X)$ and $b(X)$, and the fact that $p_\theta(\theta) = 0$ translates into considering polynomial operations modulo $p_\theta(X)$.

One of the first goals of algebraic number theory was to study the solutions of polynomial equations with coefficients in $\mathbb{Z}$. Given the equation

$$a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 = 0, \quad a_i \in \mathbb{Z} \text{ for all } i,$$

what can we say about its solutions? It is first clear that there may be solutions not in $\mathbb{Q}$, as $\sqrt{2}$, which means that in order to find the solutions, we have to consider fields larger than $\mathbb{Q}$.

Definition 5.8. We say that $\alpha \in K$ is an *algebraic integer* if it is a root of a monic polynomial with coefficients in $\mathbb{Z}$. The set of algebraic integers of K is a ring called the *ring of integers* of K, denoted $\mathcal{O}_K$.

The fact that the algebraic integers of K form a ring is a strong result [45, p. 47], which is not so easy to prove. The natural idea that comes to mind is to find the corresponding minimal polynomial. Take $\sqrt{2}$ and 2. Both are algebraic integers of $\mathbb{Q}(\sqrt{2})$. How easy is it to find the minimal polynomial of $\sqrt{2}+2$? How easy is it to find such a polynomial in general?

In this example, it can be shown [45, p. 60] that the algebraic integers are the set $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ a, b \in \mathbb{Z}\}$. Care should be taken in generalizing this result (see Example 5.1). Note that $\mathbb{Z}[\sqrt{2}]$ is a ring since it is closed under all operations except for the inversion. For example $(2 + 2\sqrt{2})^{-1} = (\sqrt{2} - 1)/2$ does not belong to $\mathbb{Z}[\sqrt{2}]$.

Theorem 5.2. [45, p. 49] If K is a number field, then $K = \mathbb{Q}(\theta)$ for an algebraic integer $\theta \in \mathcal{O}_K$.

In other words, we can always find a primitive element which is an algebraic integer. Consequently, the minimal polynomial $p_\theta(X)$ has coefficients in $\mathbb{Z}$.

5.2 Integral Basis and Canonical Embedding

In the following, we will first look at the structure of $\mathcal{O}_K$, the ring of integers of a number field. We will also define two invariants of a number field: the *discriminant* and the *signature*.

In the special case $K = \mathbb{Q}(\sqrt{2})$, we have seen that $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$, which means that $\mathcal{O}_K$ has a basis over $\mathbb{Z}$ given by $\{1, \sqrt{2}\}$. We call $\mathcal{O}_K$ a $\mathbb{Z}$*–module*. The notion of A–module, where A is a ring, is a generalization of K–vector space, where K is a field. In our case, we have that K has a structure of vector space over the field $\mathbb{Q}$, while we only have a structure of module for $\mathcal{O}_K$ over the ring $\mathbb{Z}$. This is formalized as follows:

Theorem 5.3. [45, p. 51] Let K be a number field of degree n. The ring of integers $\mathcal{O}_K$ of K forms a free $\mathbb{Z}$–module of rank n (that is, there exists a basis of n elements over $\mathbb{Z}$).

Definition 5.9. Let $\{\omega_i\}_{i=1}^n$ be a basis of the $\mathbb{Z}$–module $\mathcal{O}_K$, so that we can uniquely write any element of $\mathcal{O}_K$ as $\sum_{i=1}^n a_i\omega_i$ with $a_i \in \mathbb{Z}$ for all i. We say that $\{\omega_i\}_{i=1}^n$ is an *integral basis* of K.

We give another example of number field, where we summarize the different notions seen so far.

Example 5.1. Take $K = \mathbb{Q}(\sqrt{5})$. We know that any algebraic integer β in K has the form $a + b\sqrt{5}$ with some $a, b \in \mathbb{Q}$, such that the polynomial $p_\beta(X) = X^2 - 2aX + a^2 - 5b^2$ has integer coefficients. By simple arguments it can be shown that all the elements of $\mathcal{O}_K$ take the form $\beta = (u + v\sqrt{5})/2$ with both u, v integers with the same parity. So we can write $\beta = h + k(1 + \sqrt{5})/2$ with $h, k \in \mathbb{Z}$. This shows that $\{1, (1 + \sqrt{5})/2\}$ is an integral basis. The basis $\{1, \sqrt{5}\}$ is not integral since $a+b\sqrt{5}$ with $a, b \in \mathbb{Z}$ is only a subset of $\mathcal{O}_K$. Note that $(1+\sqrt{5})/2$ is also a primitive element of K with minimal polynomial $X^2 - X - 1$.

We will now see how a number field K can be represented, we say *embedded*, into $\mathbb{C}$.

Definition 5.10. Let $K/\mathbb{Q}$ and $L/\mathbb{Q}$ be two field extensions of $\mathbb{Q}$. We call $\varphi : K \to L$ a $\mathbb{Q}$–*homomorphism* if φ is a ring homomorphism that satisfies $\varphi(a) = a$ for all $a \in \mathbb{Q}$, i.e., that fixes $\mathbb{Q}$. Recall that if A and B are rings, a *ring homomorphism* is a map $\psi : A \to B$ that satisfies, for all $a, b \in A$

(1) $\psi(a + b) = \psi(a) + \psi(b)$
(2) $\psi(a \cdot b) = \psi(a) \cdot \psi(b)$
(3) $\psi(1) = 1$.

Definition 5.11. A $\mathbb{Q}$–homomorphism $\varphi : K \to \mathbb{C}$ is called an *embedding* of K into $\mathbb{C}$.

Note that the embedding is an injective map, so that we can really understand it as a way of representing elements of K as complex numbers.

Theorem 5.4. [45, p. 41] Let $K = \mathbb{Q}(\theta)$ be a number field of degree n over $\mathbb{Q}$. There are exactly n embeddings of K into $\mathbb{C}$: $\sigma_i : K \to \mathbb{C}$, $i = 1, \ldots, n$, defined by $\sigma_i(\theta) = \theta_i$, where θ_i are the distinct zeros in $\mathbb{C}$ of the minimum polynomial of θ over $\mathbb{Q}$.

Notice that $\sigma_1(\theta) = \theta_1 = \theta$ and thus σ_1 is the identity map, $\sigma_1(K) = K$. When we apply the embedding σ_i to an arbitrary element x of K, $x = \sum_{k=1}^{n} a_k \theta^k$, $a_k \in \mathbb{Q}$, we get, using the properties of $\mathbb{Q}$-homomorphisms

$$\begin{aligned} \sigma_i(\alpha) &= \sigma_i(\textstyle\sum_{k=1}^{n} a_k \theta^k), \quad a_k \in \mathbb{Q} \\ &= \textstyle\sum_{k=1}^{n} \sigma_i(a_k)\sigma_i(\theta)^k = \sum_{k=1}^{n} a_k \theta_i^k \in \mathbb{C} \end{aligned}$$

and we see that the image of any x under σ_i is uniquely identified by θ_i.

With the notion of embeddings, we define two quantities that will appear to be very useful when considering algebraic lattices, namely the *norm* and the *trace* of an algebraic element.

Definition 5.12. Let $x \in K$. The elements $\sigma_1(x), \sigma_2(x), \ldots \sigma_n(x)$ are called the *conjugates* of x and

$$N(x) = \prod_{i=1}^{n} \sigma_i(x), \quad \mathrm{Tr}(x) = \sum_{i=1}^{n} \sigma_i(x)$$

are called respectively the *norm* and the *trace* of x.

If the context is not clear, we write $\mathrm{Tr}_{K/\mathbb{Q}}$ resp. $N_{K/\mathbb{Q}}$ to avoid ambiguity .

Theorem 5.5. [45, p. 54] For any $x \in K$, we have $N(x)$ and $\mathrm{Tr}(x) \in \mathbb{Q}$. If $x \in \mathcal{O}_K$, we have $N(x)$ and $\mathrm{Tr}(x) \in \mathbb{Z}$.

Let us come back to the example of $\mathbb{Q}(\sqrt{2})$, and illustrate these new definitions. The roots of the minimal polynomial $X^2 - 2$ are $\theta_1 = \sqrt{2}$ and $\theta_2 = -\sqrt{2}$. Thus

$$\sigma_1(\theta) = \sqrt{2} \quad \text{and} \quad \sigma_2(\theta) = -\sqrt{2}$$

and for $x \in \mathbb{Q}(\sqrt{2})$, $x = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$

$$\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2} \quad \text{and} \quad \sigma_2(a + b\sqrt{2}) = a - b\sqrt{2} \ .$$

The norm of x is $N(x) = \sigma_1(x)\sigma_2(x) = a^2 - 2b^2$, while its trace is $\mathrm{Tr}(x) = \sigma_1(x) + \sigma_2(x) = 2a$.

These field embeddings enable to define a first *invariant* of a number field, that is a property of the field that does not depend on the way it is represented.

Definition 5.13. Let $\{\omega_1, \omega_2, \ldots \omega_n\}$ be an integral basis of K. The *discriminant* of K is defined as $d_K = \det[(\sigma_j(\omega_i))_{i,j=1}^n]^2$.

It can be shown that the discriminant is independent of the choice of a basis [43].

Theorem 5.6. [45, p. 51] The discriminant d_K of a number field belongs to $\mathbb{Z}$.

Let us compute the discriminant d_K of the field $\mathbb{Q}(\sqrt{5})$. Applying the two $\mathbb{Q}$-homomorphisms to the integral basis $\{\omega_1, \omega_2\} = \{1, (1+\sqrt{5})/2\}$, we obtain

$$d_K = \det \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{pmatrix}^2 = \det \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{pmatrix}^2 = 5 \ .$$

We now define a second invariant of a number field.

Definition 5.14. Let $\{\sigma_1, \sigma_2, \dots \sigma_n\}$ be the n embeddings of K into $\mathbb{C}$. Let r_1 be the number of embeddings with image in $\mathbb{R}$, the field of real numbers, and $2r_2$ the number of embeddings with image in $\mathbb{C}$ so that

$$r_1 + 2r_2 = n \ .$$

The pair (r_1, r_2) is called the *signature* of K. If $r_2 = 0$ we have a *totally real* algebraic number field. If $r_1 = 0$ we have a *totally complex* algebraic number field.

All the previous examples were totally real algebraic number fields with $r_1 = n$. Let us now consider $K = \mathbb{Q}(\sqrt{-3})$. The minimal polynomial of $\sqrt{-3}$ is $X^2 + 3$ and has 2 complex roots so that the signature of K is (0, 1). Observe that $\{1, \sqrt{-3}\}$ is not an integral basis. If we take $j = e^{2\pi i/3} = (-1 + i\sqrt{3})/2$ where $i = \sqrt{-1}$, we have $K = \mathbb{Q}(j) = \mathbb{Q}(\sqrt{-3})$ and an integral basis is $\{1, j\}$. The minimal polynomial of θ is $X^2 + X + 1$. The ring of integers of this field is also known as the *Eisenstein integers* ring.

We end this section with a key definition for the construction of algebraic lattices.

Definition 5.15. Let us order the σ_i's so that, for all $x \in K$, $\sigma_i(x) \in \mathbb{R}$, $1 \leq i \leq r_1$, and $\sigma_{j+r_2}(x)$ is the complex conjugate of $\sigma_j(x)$ for $r_1 + 1 \leq j \leq r_1 + r_2$. We call *canonical embedding* $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ the homomorphism defined by

$$\sigma(x) = (\sigma_1(x) \dots \sigma_{r_1}(x), \sigma_{r_1+1}(x), \dots \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \ .$$

If we identify $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $\mathbb{R}^n$, the canonical embedding can be rewritten as $\sigma : K \to \mathbb{R}^n$

$$\begin{aligned} \sigma(x) \ = \ & (\sigma_1(x), \dots \sigma_{r_1}(x), \\ & \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \dots \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)) \in \mathbb{R}^n \end{aligned}$$

where $\Re$ denotes the real part and $\Im$ the imaginary part.

The canonical embedding gives a geometrical representation of a number field, the one that will serve our purpose.

5.3 Algebraic Lattices

We are now ready to introduce algebraic lattices. The definition of canonical embedding (Definition 5.15) establishes a one-to-one correspondence between the elements of an algebraic number field of degree n and the vectors of the n-dimensional Euclidean space. The final step for constructing an algebraic lattice is given by the following result.

Theorem 5.7. [45, p. 155] Let $\{\omega_1, \omega_2, \ldots \omega_n\}$ be an integral basis of K. The n vectors $\mathbf{v}_i = \sigma(\omega_i) \in \mathbb{R}^n$, $i = 1, \ldots, n$ are linearly independent, so they define a full rank algebraic lattice $\Lambda = \Lambda(\mathcal{O}_K) = \sigma(\mathcal{O}_K)$.

Recall (Definition 3.5) that the lattice $\Lambda = \sigma(\mathcal{O}_K)$ can be expressed by means of its generator matrix M.

$$\Lambda = \{\mathbf{x} = \boldsymbol{\lambda} M \ \in \mathbb{R}^n \mid \boldsymbol{\lambda} \in \mathbb{Z}^n\}$$

The lattice generator matrix M is given explicitly by

$$\begin{pmatrix} \sigma_1(\omega_1) & \ldots & \sigma_{r_1}(\omega_1) & \Re\sigma_{r_1+1}(\omega_1) & \Im\sigma_{r_1+1}(\omega_1) & \ldots & \Re\sigma_{r_1+r_2}(\omega_1) & \Im\sigma_{r_1+r_2}(\omega_1) \\ \sigma_1(\omega_2) & \ldots & \sigma_{r_1}(\omega_2) & \Re\sigma_{r_1+1}(\omega_2) & \Im\sigma_{r_1+1}(\omega_2) & \ldots & \Re\sigma_{r_1+r_2}(\omega_2) & \Im\sigma_{r_1+r_2}(\omega_2) \\ & & & & \vdots & & & \\ \sigma_1(\omega_n) & \ldots & \sigma_{r_1}(\omega_n) & \Re\sigma_{r_1+1}(\omega_n) & \Im\sigma_{r_1+1}(\omega_n) & \ldots & \Re\sigma_{r_1+r_2}(\omega_n) & \Im\sigma_{r_1+r_2}(\omega_n) \end{pmatrix} \tag{5.1}$$

where the vectors $\mathbf{v}_i$ are the rows of M.

Given the above lattice generator matrix, it is easy to compute the determinant of the lattice.

Theorem 5.8. [43] Let d_K be the discriminant of K. The volume of the fundamental parallelotope of Λ is given by

$$vol(\Lambda) = |\det(M)| = 2^{-r_2}\sqrt{|d_K|}\ . \tag{5.2}$$

Consequently,

$$\det(\Lambda) = 2^{-2r_2}|d_K|.$$

Before going further, let us take some time to emphasize the correspondence between a lattice point $\mathbf{x} \in \Lambda \subset \mathbb{R}^n$ and an algebraic integer in $\mathcal{O}_K$. A lattice point is of the form

$$\mathbf{x} \ = \ (x_1, \ldots, x_{r_1}, x_{r_1+1}, \ldots, x_{r_1+2r_2})$$

$$= (\sum_{i=1}^{n} \lambda_i \sigma_1(\omega_i), \ldots, \sum_{i=1}^{n} \lambda_i \Re\sigma_{r_1+1}(\omega_i), \ldots, \sum_{i=1}^{n} \lambda_i \Im\sigma_{r_2+r_1}(\omega_i))$$
$$= (\sigma_1(\sum_{i=1}^{n} \lambda_i \omega_i), \ldots, \Re\sigma_{r_1+1}(\sum_{i=1}^{n} \lambda_i \omega_i), \ldots, \Im\sigma_{r_2+r_1}(\sum_{i=1}^{n} \lambda_i \omega_i))$$

for some $\lambda_i \in \mathbb{Z}$. Thus

$$\mathbf{x} = (\sigma_1(x), \ldots, \Re\sigma_{r_1+1}(x), \ldots, \Im\sigma_{r_1+r_1}(x)) = \sigma(x) \tag{5.3}$$

for $x = \sum_{i=1}^{n} \lambda_i \omega_i$ an algebraic integer. This correspondence between a vector $\mathbf{x}$ in $\mathbb{R}^n$ and an algebraic integer x in $\mathcal{O}_K$ makes it easy to compute the diversity of algebraic lattices.

Theorem 5.9. [18] Algebraic lattices exhibit a diversity

$$L = r_1 + r_2.$$

Proof. Let $\mathbf{x} \neq \mathbf{0}$ be an arbitrary point of Λ:

$$\mathbf{x} = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \ldots, \Im\sigma_{r_1+r_1}(x))$$

with $x \in \mathcal{O}_K$. Since $\mathbf{x} \neq \mathbf{0}$, we have $x \neq 0$ and the first r_1 coefficients are non-zero. The minimum number of non-zero coefficients among the $2r_2$ that are left is r_2 since the real and imaginary parts of any one of the complex embeddings may not be null together. We thus have a diversity $L \geq r_1 + r_2$. Applying the canonical embedding to $x = 1$ gives exactly $r_1 + r_2$ non-zero coefficients ($\sigma_j(1) = 1$ for any j), which concludes the proof. □

Corollary 5.1. Algebraic lattices built over totally real number fields (that is with signature $(r_1, r_2) = (n, 0)$) have maximal diversity $L = n$.

Example 5.2. Figure 5.1 shows an algebraic lattice from $K = \mathbb{Q}(\sqrt{5})$. As seen before, the integral basis of K is $\{1, \frac{1+\sqrt{5}}{2}\}$. The two embeddings are $\sigma_1(\sqrt{5}) = \sqrt{5}$, $\sigma_2(\sqrt{5}) = -\sqrt{5}$ and the lattice generator matrix becomes

$$M = \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{pmatrix}.$$

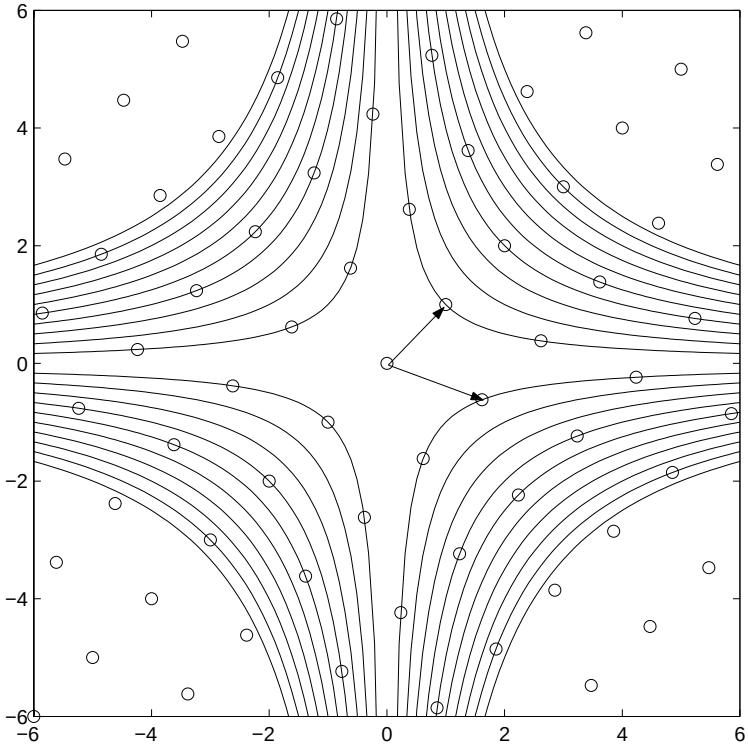

Fig. 5.1 Algebraic lattice from $\mathbb{Q}(\sqrt{5})$.

The fundamental volume is $vol(\Lambda(\mathcal{O}_K)) = |\det(M)| = \sqrt{5}$, $r_1 = 2, r_2 = 0$ and the diversity is $L = 2$. We note from Fig. 5.1 that all lattice points are on one of the hyperboles $XY = k$ for some integer $k \neq 0$, since we have that the corresponding algebraic integer has a norm equal to k.

Example 5.3. Let us consider the field $K = \mathbb{Q}(\theta)$, where θ is a primitive element with minimal polynomial $X^3 - X - 1$, whose roots are

$$\theta_1 = U + V \quad \theta_{2,3} = -\frac{1}{2}(U+V) \pm i\frac{\sqrt{3}}{2}(U-V)$$

where

$$U = \frac{1}{3}\sqrt[3]{\frac{9+3\sqrt{63}}{2}} \qquad V = \frac{1}{3}\sqrt[3]{\frac{9-3\sqrt{63}}{2}}\ .$$

The primitive element θ coincides with θ_2 and an integral basis is $\{1, \theta, \theta^2\}$. The three embeddings are $\sigma_1(\theta) = \theta_1$ (real), $\sigma_2(\theta) = \theta_2$ and $\sigma_3(\theta) = \theta_3$, where σ_2 and σ_3 are conjugates ($r_1 = 1, r_2 = 1$). We obtain the lattice generator matrix:

$$M = \begin{pmatrix} 1 & 1 & 0 \\ (U+V) & -\frac{1}{2}(U+V) & \frac{\sqrt{3}}{2}(U+V) \\ (U+V)^2 - 4 & -\frac{1}{2}(U^2+V^2-4UV) & -\frac{\sqrt{3}}{2}(U^2-V^2) \end{pmatrix}$$
$$= \begin{pmatrix} 1.000 & 1.000 & 0.000 \\ 1.325 & -0.662 & 0.562 \\ 1.755 & 0.123 & -0.745 \end{pmatrix}.$$

The fundamental volume is $vol(\Lambda(\mathcal{O}_K)) = |\det(M)| = 2.39$. The diversity is given by $L = r_1 + r_2 = 2$, since the vector $(1, 1, 0)$ belongs to the lattice and $d_p^{(2)}((0,0,0),(1,1,0)) = 1$.

So far, the key ingredient to build an algebraic lattice has been the existence of a $\mathbb{Z}$-basis in K. Since it is known that $\mathcal{O}_K$ has such basis (more technically that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n), we can embed it into $\mathbb{R}^n$ so as to obtain an algebraic lattice. However, there exist other subsets of $\mathcal{O}_K$ that also have this structure of free $\mathbb{Z}$-module of rank n. These are the *ideals* of $\mathcal{O}_K$.

Definition 5.16. An *ideal* $\mathcal{I}$ of a commutative ring R is an additive subgroup of R which is stable under multiplication by R, i.e., $a\mathcal{I} \subseteq \mathcal{I}$ for all $a \in R$.

Among all the ideals of a ring, some of them have the special property of being generated by only one element. These will be of particular interest for us.

Definition 5.17. An ideal $\mathcal{I}$ of R is *principal* if it is of the form $\mathcal{I} = (x) = (x)R = \{xy,\ y \in R\}$, $x \in \mathcal{I}$.

Example 5.4. If $R = \mathbb{Z}$, we have that $n\mathbb{Z}$ is a principal ideal of $\mathbb{Z}$ for all n.

We can define the *norm* of an ideal. In the case where the ideal is principal, it is directly related to the norm of a generator of the ideal.

Definition 5.18. Let $\mathcal{I} = (x)\mathcal{O}_K$ be a principal ideal of $\mathcal{O}_K$. Its *norm* is defined by $N(\mathcal{I}) = |N(x)|$.

It can be shown that all ideals of $\mathcal{O}_K$ have a $\mathbb{Z}$-basis of n elements.

Theorem 5.10. [45, p. 121] Every ideal $\mathcal{I} \neq \{0\}$ of $\mathcal{O}_K$ has a $\mathbb{Z}$-basis $\{\nu_1, \ldots, \nu_n\}$ where n is the degree of K.

Theorems 5.7 and 5.9 easily extend when replacing a basis of $\mathcal{O}_K$ by a basis of $\mathcal{I} \subseteq \mathcal{O}_K$. An algebraic lattice Λ' built from an ideal $\mathcal{I} \subseteq \mathcal{O}_K$ gives a sublattice of the algebraic lattice Λ built from $\mathcal{O}_K$.

Theorem 5.11. [43] The volume of the fundamental parallelotope of Λ' is given by

$$vol(\Lambda') = |\det(M)| = 2^{-r_2} N(\mathcal{I}) \cdot \sqrt{|d_K|} \tag{5.4}$$

5.4 Algebraic Lattices over Totally Real Number Fields

All the theory seen so far may be applied to number fields with arbitrary signature. Since we are interested in obtaining the maximal diversity, we concentrate on totally real number fields (see Corollary 5.1). Furthermore, we will see that the minimum product distance can be easily computed in this case.

Let K be a totally real number field of degree n, and let $\Lambda(\mathcal{O}_K)$ be an algebraic lattice built over $\mathcal{O}_K$. Then its lattice generator simplifies to

$$M = \begin{pmatrix} \sigma_1(\omega_1) & \sigma_2(\omega_1) & \ldots & \sigma_n(\omega_1) \\ \sigma_1(\omega_2) & \sigma_2(\omega_2) & \ldots & \sigma_n(\omega_2) \\ \vdots & & & \vdots \\ \sigma_1(\omega_n) & \sigma_2(\omega_n) & \ldots & \sigma_n(\omega_n) \end{pmatrix}.$$

The product distance of $\mathbf{x}$ from $\mathbf{0}$ is related to the algebraic norm [18]:

$$d_p^{(n)}(\mathbf{0}, \mathbf{x}) = \prod_{j=1}^{n} |\mathbf{x}_j| = \prod_{j=1}^{n} |\sigma_j(x)| = |N(x)|$$

with $x \in \mathcal{O}_K$. Note that for algebraic lattices from arbitrary number fields with signature (r_1, r_2), with generator matrix (5.1), the product distance cannot be related to the algebraic norm.

Since $x \neq 0$, we have by Theorem 5.5

$$d_p^{(n)}(\mathbf{0}, \mathbf{x}) \geq 1 \qquad \forall\, \mathbf{x} \neq \mathbf{0}\ .$$

The minimum product distance of the algebraic lattice $\Lambda(\mathcal{O}_K)$ is thus

$$d_{p,min}(\Lambda(\mathcal{O}_K)) = 1.$$

In order to compare $d_{p,min}$'s of different lattices we will conveniently normalize the fundamental volume of the lattice to one. In the next section we show how this result on the product distance can be extended to the family of *ideal lattices*.

5.5 Appendix: First Commands in KASH/KANT

This section is for readers interested in implementing the computations of the examples with a computer algebra system. The use of such a program is very helpful, since all the environment for working over number fields is easily defined. Several computational algebra packages are available [40, 2]. Here we choose the computer algebra freeware KASH/KANT [40, 24].

Example of $\mathbb{Q}(\sqrt{2})$

The first thing to know is that we work over $K = \mathbb{Q}(\sqrt{2})$ via its ring of integers $\mathcal{O}_K$. In order to define it, we use its minimal polynomial. In general, a polynomial is given by specifying over which ring it is defined, and which are its coefficients. The command `Zx` means that the polynomial has coefficients in $\mathbb{Z}$.

```
# define the minimal polynomial
kash> p2 := Poly(Zx,[1,0,-2]);
x^2 - 2
```

We are now ready to define $\mathcal{O}_K$. Note that the command `OrderMaximal` returns the ring of integers. We then ask for a basis of $\mathcal{O}_K$, i.e., for an integral basis of K.

```
# define the ring of integers of Q(sqrt{2})
kash> O2 := OrderMaximal(p2);
```

```
Generating polynomial: x^2 - 2
Discriminant: 8

# ask for an integral basis
kash> OrderBasis(O2);
[ 1, [0, 1] ]
```

Note that the basis is given with respect to the $\mathbb{Q}$-basis, which is $\{1, \sqrt{2}\}$, since the minimal polynomial is $X^2 - 2$. Thus $[a, b]$ stands for $a + b\sqrt{2}$.

```
# compute the embeddings
kash> OrderAutomorphisms(O2);
[ [0, 1], [0, -1] ]
```

The first embedding is the identity, the second maps $\sqrt{2}$ onto $-\sqrt{2}$.

Example of $\mathbb{Q}(\sqrt{5})$

Similarly as in the example of $\mathbb{Q}(\sqrt{2})$, we define and work on the ring of integers of $\mathbb{Q}(\sqrt{5})$.

```
# define the minimal polynomial
kash> p5 := Poly(Zx,[1,0,-5]);
x^2 - 5

# define the ring of integers of Q(sqrt{5})
kash> O5 := OrderMaximal(p5);
   F[1]
    |
   F[2]
  /
 /
Q
F  [ 1]     Given by transformation matrix
F  [ 2]     x^2 - 5
Discriminant: 5
```

```
# The same ring of integers can be obtained as follows.
kash> OrderMaximal(Poly(Zx,[1,1,-1]));
Generating polynomial: x^2 + x - 1
Discriminant: 5

# ask for an integral basis
kash> OrderBasis(O5);
[ 1, [1, 1] / 2 ]
```

Again, the basis is given with respect to the $\mathbb{Q}$-basis, which is $\{1, \sqrt{5}\}$. Thus the second element of the basis is $(1+\sqrt{5})/2$. Note that the choice of an integral basis is not unique and the way it is computed depends on the choice of a minimal polynomial. In the case the polynomial is $X^2 + X - 1$, we have

```
kash> OrderBasis(OrderMaximal(Poly(Zx,[1,1,-1])));
[ 1, [0, 1] ]
```

where the $\mathbb{Q}$-basis is this time $\{1, (-1 + \sqrt{5})/2)\}$ with $(-1 + \sqrt{5})/2$ a root of the minimal polynomial.

Remark 5.3. The integral basis of $\mathbb{Q}(\sqrt{5})$ is not $\{1, \sqrt{5}\}$ as one may expect referring to the previous example where the integral basis of $\mathbb{Q}(\sqrt{2})$ is $\{1, \sqrt{2}\}$.

```
# compute the embeddings
kash> OrderAutomorphisms(O5);
[ [-1, 2], [1, -2] ]
```

Be careful that here the embeddings are given in the basis of the ring of integers. Thus $[-1, 2] = -1 + 2(1 + \sqrt{5})/2 = \sqrt{5}$. This represents the first embedding, which is the identity. The other maps $\sqrt{5}$ to $-\sqrt{5}$.

```
# write the second element of the integral basis
kash> b:= Elt(O5,[0,1]);
[0, 1]
```

After executing the command `OrderAutomorphisms`, KASH/KANT has in memory the different embeddings, so that it is possible to call one of them, and to apply it on an element. The command `EltAutomorphism(b,n)` computes a conjugate of the element b, applying on it the nth embedding.

```
# compute the generator matrix of the lattice
kash> M5:=Mat(O5,[[1,1],[b,EltAutomorphism(b,2)]]);
[1 1]
[[0, 1] [1, -1]]

# compute its determinant
kash> MatDet(M5);
[1, -2]
```

One can easily check that the determinant is $-\sqrt{5}$ as expected. The generator matrix can be obtained directly with the command `Lat`.

```
kash> Lat(O5);
Basis:
[1 -0.6180339887498948482045868343656381177203091798 06]
[1 1.6180339887498948482045868343656381177203091798 06]
```

Example of $\mathbb{Q}(\sqrt{-3})$

This example follows the steps of the two previous examples.

```
# define the minimal polynomial
kash> p3 := Poly(Zx,[1,0,3]);
x^2 + 3

# define the ring of integers of Q(sqrt{-3})
kash> O3:=OrderMaximal(p3);
   F[1]
    |
   F[2]
  /
 /
```

```
Q
F  [ 1]     Given by transformation matrix
F  [ 2]     x^2 + 3
Discriminant: -3

# The same ring of integers can be obtained as follows.
kash> OrderMaximal(Poly(Zx,[1,-1,1]));
Generating polynomial: x^2 - x + 1
Discriminant: -3

# ask for an integral basis
kash> OrderBasis(O3);
[ 1, [1, 1] / 2 ]

# compute the embeddings
kash> OrderAutomorphisms(O3);
[ [-1, 2], [1, -2] ]
```

6

Ideal Lattices

In this section we study a family of algebraic lattices endowed with a *trace form* called *ideal lattices*. Ideal lattices describe lattices with a generator matrix of the type $M = (\sigma_i(\omega_j))_{i,j=1}^n \cdot A$, where A is a convenient diagonal matrix. We can think of the diagonal matrix A as a pre-fading, used to stretch an algebraic lattice into another, such as the $\mathbb{Z}^n$–lattice. We will restrict ourselves to totally real number fields in order to have maximum diversity. We will show how to derive an explicit formula for the minimum product distance. Furthermore, we will discuss the basic ideas for the construction of full-diversity rotated $\mathbb{Z}^n$–lattices from ideal lattices, which will be developed in Section 7.

6.1 Definition and Minimum Product Distance of an Ideal Lattice

In the following, K will denote a totally real number field of degree n. Let $\{\sigma_i\}_{i=1}^n$ denote the n real embeddings of K into $\mathbb{C}$.

Definition 6.1. An *ideal lattice* is a lattice $\Lambda = (\mathcal{I}, q_\alpha)$, where $\mathcal{I} \subseteq \mathcal{O}_K$ is an ideal of $\mathcal{O}_K$ and

$$q_\alpha : \mathcal{I} \times \mathcal{I} \to \mathbb{Z}, \quad q_\alpha(x, y) = \mathrm{Tr}(\alpha x y), \quad \forall x, y \in \mathcal{I}$$

where $\alpha \in K$ is totally positive (i.e. $\sigma_i(\alpha) > 0,\ \forall i$).

Let $\{\omega_1, \ldots, \omega_n\}$ be a $\mathbb{Z}$-basis of the above ideal $\mathcal{I} \subseteq \mathcal{O}_K$. Using the above notations, we define a *twisted canonical embedding* $\sigma_\alpha : K \to \mathbb{R}^n$ as

$$\sigma_\alpha(x) = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_n}\sigma_n(x))$$

where $\alpha_i = \sigma_i(\alpha)$, $i = 1, \ldots, n$.

Using the twisted canonical embedding the generator matrix M of the lattice $\Lambda = \sigma_\alpha(\mathcal{I})$ is given by

$$\begin{aligned} M &= \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(\omega_1) & \sqrt{\alpha_2}\sigma_2(\omega_1) & \ldots & \sqrt{\alpha_n}\sigma_n(\omega_1) \\ \vdots & \vdots & \ldots & \vdots \\ \sqrt{\alpha_1}\sigma_1(\omega_n) & \sqrt{\alpha_2}\sigma_2(\omega_n) & \ldots & \sqrt{\alpha_n}\sigma_n(\omega_n) \end{pmatrix} \\ &= (\sigma_i(\omega_j))_{i,j=1}^n \begin{pmatrix} \sqrt{\alpha_1} & & 0 \\ & \ddots & \\ 0 & & \sqrt{\alpha_n} \end{pmatrix} . \end{aligned} \tag{6.1}$$

The corresponding Gram matrix G is given by $G = MM^T = (g_{ij})_{i,j=1}^n$ where

$$\begin{aligned} g_{ij} &= \sum_{k=1}^{n} \sqrt{\alpha_k}\sigma_k(\omega_i)\sqrt{\alpha_k}\sigma_k(\omega_j) \\ &= \sum_{k=1}^{n} \alpha_k \sigma_k(\omega_i\omega_j) \\ &= \mathrm{Tr}(\alpha\, \omega_i\omega_j) \ . \end{aligned}$$

Since the Gram matrix is a trace form, this shows that the generator matrix as given above indeed defines an ideal lattice. In the case of ideal lattices, the determinant of the lattice is related both to the discriminant d_K and to the norm of the ideal $\mathcal{I}$.

Proposition 6.1. [3] Let $\mathcal{I}$ be an ideal of $\mathcal{O}_K$, and $\Lambda = (\mathcal{I}, q_\alpha)$ be an ideal lattice. Then

$$\det(\Lambda) = N(\alpha)N(\mathcal{I})^2|d_K|.$$

The minimum product distance of an ideal lattice can be computed explicitly when the ideal is principal.

Lemma 6.1. If $\mathcal{I}$ is a principal ideal of $\mathcal{O}_K$, then

$$\min_{x \neq 0 \in \mathcal{I}} N(x) = N(\mathcal{I}).$$

Proof. Since $\mathcal{I}$ is principal, $\mathcal{I} = (a)$, for $a \in \mathcal{I}$, and $N(\mathcal{I}) = |N(a)|$ (see Definition 5.18). Let $x \in \mathcal{I}$, so that $x = ay$ for some $y \in \mathcal{O}_K$. Thus $|N(x)| = |N(a)||N(y)| \geq N(\mathcal{I})$ and equality holds if and only if $N(y) = \pm 1$. The minimum is reached, taking for example $y = 1$. □

Exactly in the same way as for algebraic lattices (see Equation (5.3)), there is a correspondence between a point $\mathbf{x} \in \Lambda = (\mathcal{I}, q_\alpha) \subseteq \mathbb{R}^n$ and an algebraic integer:

$$\begin{aligned} \mathbf{x} &= (\sum_{i=1}^{n} \lambda_i \sqrt{\alpha_1} \sigma_1(\omega_i), \ldots, \sum_{i=1}^{n} \lambda_i \sqrt{\alpha_n} \sigma_n(\omega_i)), \ \lambda_i \in \mathbb{Z} \\ &= \sigma_\alpha(x) \end{aligned}$$

for $x \in \mathcal{I} \subseteq \mathcal{O}_K$.

Theorem 6.1. Let $\mathcal{I}$ be a principal ideal of $\mathcal{O}_K$. The minimum product distance of an ideal lattice $\Lambda = (\mathcal{I}, q_\alpha)$ is

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{d_K}}.$$

Proof. Let $\mathbf{x}$ be a lattice point and $x \in \mathcal{I}$ be its corresponding algebraic integer, so that $\mathbf{x} = \sigma_\alpha(x)$. We have:

$$\begin{aligned} d_{p,min}(\Lambda) &= \min_{\mathbf{x} \neq \mathbf{0} \in \Lambda} \prod_{j=1}^{n} |x_j| = \min_{x \neq 0 \in \mathcal{I}} \prod_{j=1}^{n} |\sqrt{\alpha_j} \sigma_j(x)| \\ &= \sqrt{N(\alpha)} \min_{x \neq 0 \in \mathcal{I}} |N(x)|. \end{aligned}$$

We conclude using Proposition 6.1 and Lemma 6.1.

$$d_{p,min}(\Lambda) = \sqrt{N(\alpha)} \min_{x \neq 0 \in I} N(x) = \sqrt{\frac{\det(\Lambda)}{d_K}}.$$

□

Less explicit results are available in the case of non-principal ideals [39]. The corresponding ideal lattices are conjectured to have a lower $d_{p,min}$.

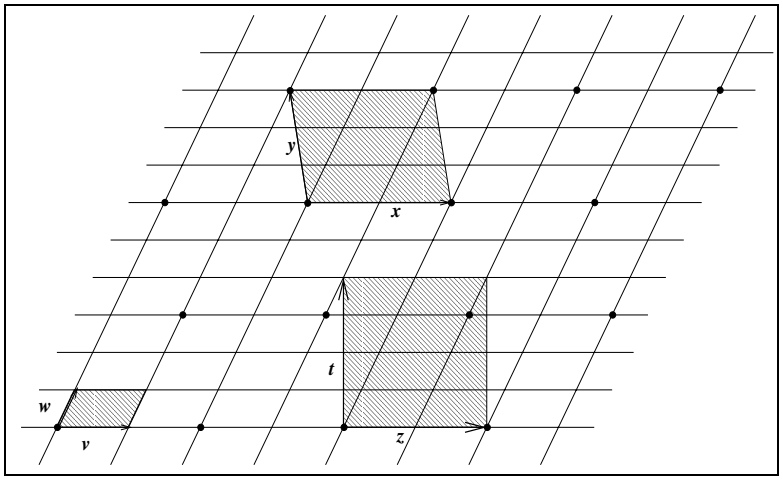

Fig. 6.1 Looking for a square sublattice in a given lattice: the lattice Λ has basis $\{\mathbf{v}, \mathbf{w}\}$, while its sublattices Λ' and Λ'' have bases $\{\mathbf{t}, \mathbf{z}\}$, resp. $\{\mathbf{x}, \mathbf{y}\}$. The lattice Λ' is a square lattice.

6.2 $\mathbb{Z}^n$ Ideal Lattices

We focus now on the construction of a particular lattice: $\mathbb{Z}^n$, $n \geq 2$. In terms of ideal lattices, this means that, given n, we are looking for a number field K of degree n and an ideal $\mathcal{I} \subseteq \mathcal{O}_K$ such that $\Lambda = (\mathcal{I}, q_\alpha)$ is equivalent to $\mathbb{Z}^n$, $n \geq 2$. The Gram matrix G of this lattice is the identity matrix, so that the lattice generator matrix M is an orthogonal matrix: $MM^T = I_n$. From a geometrical point of view, a lattice $\Lambda' = (\mathcal{I}, q_\alpha)$ over $\mathcal{I} \subseteq \mathcal{O}_K$ is a sublattice of $\Lambda = (\mathcal{O}_K, q_\alpha)$. The idea is thus that in a given lattice Λ, there may be a sublattice which is $\mathbb{Z}^n$, as shown in Fig. 6.1 for $n = 2$.

The lattice determinant will be a useful criterion to help us finding the $\mathbb{Z}^n$–lattice. Recall that the determinant of $\mathbb{Z}^n$ is 1, $n \geq 2$. A scaled version of $\mathbb{Z}^n$ is of the form $(\sqrt{c}\mathbb{Z})^n$ for some integer c, so that its determinant is $\det(G) = \det(M)^2 = c^n$. Using Proposition 6.1, we deduce the following necessary (but not sufficient!) condition:

$$N(\mathcal{I})^2 N(\alpha) d_K = c^n \tag{6.2}$$

where c is an integer. If we assume $\mathcal{I} = \mathcal{O}_K$, this simplifies to

$$N(\alpha) d_K = c^n \tag{6.3}$$

while if we take $\alpha = 1$, it simplifies to

$$N(\mathcal{I})^2 d_K = c^n. \tag{6.4}$$

The necessary condition (6.2) will help us to choose α in the next section to build $\mathbb{Z}^n$–lattice codes.

7

Rotated $\mathbb{Z}^n$–lattices Codes

The question of finding algebraic lattices over totally real number fields with maximal minimum product distance has been extensively studied in the last decade.

The first examples using totally real algebraic number fields were given in [9]. Initially, no restriction on the shape of the lattice constellation was imposed, which resulted in either a complex bit labeling procedure or loss in the average energy, as explained in Section 2.4. Further investigations were addressed to finding rotated $\mathbb{Z}^n$–lattices to avoid the above problems [15, 11, 33, 17]. In [4], several families of full-diversity rotated $\mathbb{Z}^n$–lattices from totally real algebraic number fields were given and analyzed for all dimensions. In this section, we explain how to construct one of these families.

7.1 A Fully Worked Out Example

Suppose we want to build the 2-dimensional lattice $\mathbb{Z}^2$ with full diversity. We take the field $K = \mathbb{Q}(\sqrt{5})$, whose discriminant is $d_K = 5$. We know that K is totally real, since its two embeddings are

$$\sigma_1(a + b\sqrt{5}) = a + b\sqrt{5} \text{ and } \sigma_2(a + b\sqrt{5}) = a - b\sqrt{5}, \quad a, b \in \mathbb{Q}.$$

We have seen in (6.3) that a necessary condition for obtaining $\mathbb{Z}^2$ is to have an element α such that

$$N(\alpha)d_K = N(\alpha)\cdot 5 = c^2, \quad c \in \mathbb{Z}.$$

It is natural to look for an element $\alpha \in K$ whose norm is 5. It is a direct computation to check that the element

$$\alpha = 3 - \frac{1+\sqrt{5}}{2} \tag{7.1}$$

has the right norm:

$$N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = \left(3 - \frac{1+\sqrt{5}}{2}\right)\left(3 - \frac{1-\sqrt{5}}{2}\right) = 5.$$

A good choice for trying to build $\mathbb{Z}^2$ as an ideal lattice thus consists in taking $\mathcal{I} = \mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ (see Example 5.1) with α given by (7.1). The lattice generator matrix M is given by

$$M = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & \sqrt{\sigma_2(\alpha)} \\ \sqrt{\sigma_1(\alpha)}\sigma_1(\frac{1+\sqrt{5}}{2}) & \sqrt{\sigma_2(\alpha)}\sigma_2(\frac{1+\sqrt{5}}{2}) \end{pmatrix}.$$

Let us now compute the Gram matrix $G = MM^T$:

$$\begin{aligned} G &= \begin{pmatrix} \sigma_1(\alpha)+\sigma_2(\alpha) & \sigma_1(\alpha\frac{1+\sqrt{5}}{2})+\sigma_2(\alpha\frac{1+\sqrt{5}}{2}) \\ \sigma_1(\alpha\frac{1+\sqrt{5}}{2})+\sigma_2(\alpha\frac{1+\sqrt{5}}{2}) & \sigma_1(\alpha(\frac{1+\sqrt{5}}{2})^2)+\sigma_2(\alpha(\frac{1+\sqrt{5}}{2})^2) \end{pmatrix} \\ &= \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}. \end{aligned}$$

This shows that we get a scaled version of $\mathbb{Z}^2$. After normalization, we have that $\mathbb{Z}^2$ can be built over $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, with generator matrix $\frac{1}{\sqrt{5}}M$ (see Fig. 7.1). By Theorem 6.1, the minimum product distance of this lattice code is

$$d_{p,min} = \frac{1}{\sqrt{d_K}} = \frac{1}{\sqrt{5}}.$$

7.2 The Cyclotomic Construction

We give a general construction that allows us to obtain $\mathbb{Z}^n$ for $n = (p-1)/2$, $p \geq 5$ a prime. The example of the previous section will

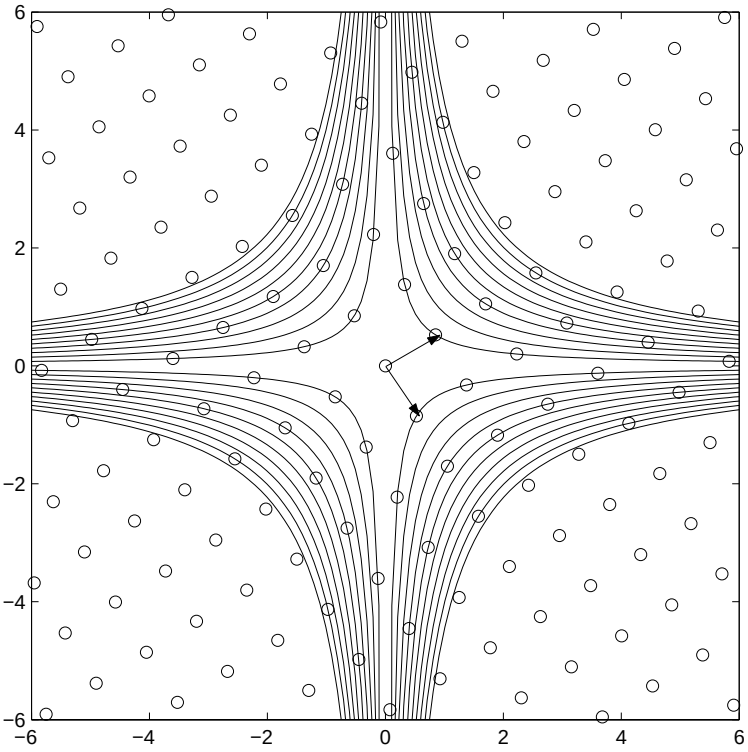

Fig. 7.1 The rotated square algebraic lattice from $\mathbb{Q}(\sqrt{5})$.

appear to be a particular case. For that, we need to introduce the so-called *cyclotomic fields* [45, 53].

Definition 7.1. A *cyclotomic field* is a number field $K = \mathbb{Q}(\zeta_m)$ generated by an m-th root of unity, $\zeta_m = e^{2i\pi/m}$.

We are interested in the particular case where $m = p \geq 5$ is a prime. The degree of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ is $p - 1$.

Definition 7.2. Let $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ be a subfield of $\mathbb{Q}(\zeta_p)$ generated by $\zeta_p + \zeta_p^{-1} = 2\cos(2\pi/p)$, where ζ_p is a pth root of unity. Since $[\mathbb{Q}(\zeta_p) : K] = 2$ and K is totally real, it is called the *maximal real subfield* of a cyclotomic field.

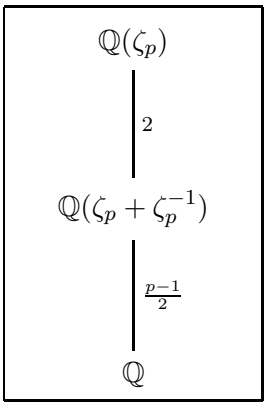

Fig. 7.2 Cyclotomic field and its maximal real subfield.

The degree of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ over $\mathbb{Q}$ is $(p-1)/2$ (see Fig. 7.2) and its discriminant is

$$d_K = p^{\frac{p-3}{2}}, \tag{7.2}$$

as it can be computed from [46, p. 46, Th. 21].

Proposition 7.1. [53, p. 16] Let $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Its ring of integers is $\mathcal{O}_K = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.

An integral basis (see Definition 5.9) of $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is given by $\{e_j = \zeta_p^j + \zeta_p^{-j}\}_{j=1}^n$. There are n embeddings of K into $\mathbb{C}$ given by

$$\sigma_k(e_j) = \zeta_p^{kj} + \zeta_p^{-kj}. \tag{7.3}$$

We recall from (6.3) that a necessary condition for obtaining the $\mathbb{Z}^n$ ideal lattice is to find an element α such that

$$N(\alpha)p^{\frac{p-3}{2}} = c^n = p^{\frac{p-1}{2}}. \tag{7.4}$$

The element $\alpha = (1-\zeta_p)(1-\zeta_p^{-1})$ has norm $N(\alpha) = p$.

The following theorem shows that using this element, we are actually able to build the $\mathbb{Z}^n$–lattice.

Theorem 7.1. Let $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and $\alpha = (1-\zeta_p)(1-\zeta_p^{-1})$. Then

$$\Lambda = (\mathcal{O}_K, \frac{1}{p} q_\alpha) \text{ is equivalent to } \mathbb{Z}^n,$$

where we recall that $q_\alpha(x, y) = \mathrm{Tr}(\alpha x y)$.

Proof. The proof is a direct computation. To simplify notation, we write $\zeta = \zeta_p$.

We first compute $\mathrm{Tr}(\alpha e_i e_j)$ where $\{e_j\}_{j=1}^n$ is the usual integral basis of $\mathbb{Q}(\zeta + \zeta^{-1})$. From the matrix that we obtain, we find a new basis $\{e'_j\}_{j=1}^n$ where $\frac{1}{p}\mathrm{Tr}(\alpha e'_i e'_j)$ is exactly the identity matrix. Let

$$\alpha = (1-\zeta)(1-\zeta^{-1}) = 2 - (\zeta + \zeta^{-1}) \tag{7.5}$$

and denote by $\sigma_j(\zeta)$ and $\alpha_j = \sigma_j(\alpha)$ for $j = 1, \ldots, n$ the conjugates of ζ and α, respectively (see (7.3)). Note that

$$\mathrm{Tr}(\zeta^k + \zeta^{-k}) = \sum_{j=1}^n \sigma_j(\zeta^k + \zeta^{-k}) = -1, \ \forall\ k = 1, \ldots, n. \tag{7.6}$$

Using (7.6) we have

$$\begin{aligned}
\sum_{j=1}^n \alpha_j \sigma_j(\zeta^k + \zeta^{-k}) &= \sum_{j=1}^n (2 - \sigma_j(\zeta + \zeta^{-1}))\sigma_j(\zeta^k + \zeta^{-k}) \\
&= -2 - \sum_{j=1}^n \sigma_j(\zeta^{k+1} + \zeta^{-k-1} + \zeta^{-k+1} + \zeta^{k-1}) \\
&= \begin{cases} = & -p \quad \text{if } k \equiv \pm 1 \pmod{p} \\ = & 0 \quad \text{otherwise.} \end{cases}
\end{aligned} \tag{7.7}$$

We now compute $q_\alpha(e_i, e_j)$ for $i = j$ and $i \neq j$ using (7.7) and (7.6).

$$\begin{aligned}
q_\alpha(e_i, e_i) &= \sum_{j=1}^n \alpha_j \sigma_j(\zeta^{2i} + \zeta^{-2i} + 2) \\
&= \sum_{j=1}^n \alpha_j \sigma_j(\zeta^{2i} + \zeta^{-2i}) + 2\sum_{j=1}^n (2 - \sigma_j(\zeta + \zeta^{-1})) \\
&= \begin{cases} p & \text{if } i = n, \text{ i.e } 2i \equiv -1 \pmod{p} \\ 2p & \text{otherwise} \end{cases} \\
q_\alpha(e_i, e_j) &= \sum_{k=1}^n \alpha_k \sigma_k(\zeta^{i+j} + \zeta^{-(i+j)}) + \sum_{k=1}^n \alpha_k \sigma_k(\zeta^{i-j} + \zeta^{-(i-j)}) \\
&= \begin{cases} -p & \text{if } |i-j| = 1 \\ 0 & \text{otherwise.} \end{cases}
\end{aligned}$$

Thus the matrix of q_α in the basis $\{e_1, \ldots, e_n\}$ is given by

$$\begin{pmatrix} 2 & -1 & 0 & & \cdots & 0 \\ -1 & 2 & -1 & & & \\ 0 & -1 & 2 & & & \\ & & & \ddots & -1 & 0 \\ & & & -1 & 2 & -1 \\ 0 & \cdots & & 0 & -1 & 1 \end{pmatrix}.$$

In the new basis $\{e'_1, \ldots, e'_n\}$, where $e'_n = e_n$ and $e'_j = e_j + e'_{j+1}$, $j = 1, \ldots, n-1$, the above matrix is the Gram matrix of the lattice $\mathbb{Z}^n$, i.e. p times the identity matrix. □

The corresponding rotated $\mathbb{Z}^n$–lattice is obtained as follows. Recall from (7.3) that the n field embeddings of K are

$$\sigma_k(e_j) = \zeta^{kj} + \zeta^{-kj} = 2\cos\left(\frac{2\pi kj}{p}\right).$$

Then the lattice generated by the ring of integers has the $n \times n$ generator matrix M with elements $M_{k,j} = 2\cos\left(\frac{2\pi kj}{p}\right)$. The element α can be represented by the diagonal matrix

$$A = \operatorname{diag}\left(\sqrt{\sigma_k(\alpha)}\right).$$

The basis transformation matrix from $\{e_j\}$ to $\{e'_j\}$ is given by

$$T = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 1 & \cdots & 1 \\ \vdots & & \ddots & & \vdots \\ 0 & \cdots & 0 & 1 & 1 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Finally, the rotated $\mathbb{Z}^n$–lattice generator matrix is given by

$$R = \frac{1}{\sqrt{p}}\, TMA.$$

Following the above recipe we obtain rotated $\mathbb{Z}^n$–lattices for $n = 2, 3, 5, 6, 8, 9, 11, 14, 15, 18,\ 20, 21, 23, 26, 29, 30, \ldots$

n	$d_{p,min}$	$\sqrt[n]{d_{p,min}}$	n	$d_{p,min}$	$\sqrt[n]{d_{p,min}}$
2	$1/\sqrt{5}$	0.668740	15	$1/31^7$	0.201386
3	$1/7$	0.522757	18	$1/\sqrt{37^{17}}$	0.181744
5	$1/11^2$	0.383215	20	$1/\sqrt{41^{19}}$	0.171367
6	$1/\sqrt{13^5}$	0.343444	21	$1/43^{10}$	0.166785
8	$1/\sqrt{17^7}$	0.289520	23	$1/47^{11}$	0.158599
9	$1/19^4$	0.270187	26	$1/\sqrt{53^{25}}$	0.148259
11	$1/23^5$	0.240454	29	$1/59^{14}$	0.139670
14	$1/\sqrt{29^{13}}$	0.209425	30	$1/\sqrt{61^{29}}$	0.137116

Table 7.1 Minimum product distances for the cyclotomic construction.

Proposition 7.2. The minimum product distance of the ideal lattice Λ of dimension n as defined in Th. 7.1 is

$$d_{p,min}(\Lambda) = p^{-\frac{n-1}{2}}.$$

Proof. By Theorem 6.1, the minimum product distance is given by $d_{p,min} = 1/\sqrt{d_K}$ since we have normalized $\det(\Lambda) = 1$. We conclude recalling (7.2) that the discriminant of K is $d_K = p^{\frac{p-3}{2}} = p^{n-1}$. □

Numerical values of $d_{p,min}$ are given in Table 7.1.

7.3 Mixed Constructions

We present a technique to combine the previous constructions to build rotated $\mathbb{Z}^n$–lattices in other dimensions.

Proposition 7.3. Let $m = p_1 \cdots p_N$ be the product of N distinct primes, $\zeta_j = e^{-i2\pi/p_j}$ for $j = 1, \ldots, N$ and K be the compositum of $K_j = \mathbb{Q}(\zeta_j + \zeta_j^{-1})$, $j = 1, \ldots, N$, (i.e., the smallest field containing all K_j). Let $\alpha_j = (1 - \zeta_j)(1 - \zeta_j^{-1})$ then

$$\Lambda = \left(\mathcal{O}_K, \frac{1}{p_1} q_{\alpha_1} \otimes \cdots \otimes \frac{1}{p_N} q_{\alpha_N} \right) \text{ is equivalent to } \mathbb{Z}^n,$$

where $n = \prod_{j=1}^{N} (p_j - 1)/2$ and $\otimes$ denotes the tensor product.

Proof. Let us consider $K = K_1K_2$. Denote by $\{\omega_1, \ldots, \omega_{n_1}\}$ and $\{\omega'_1, \ldots, \omega'_{n_2}\}$ the integral bases of K_1 and K_2, respectively. Since K_1 and K_2 have coprime discriminants, we have that

$$\{\omega_j\omega'_k \mid j = 1, \ldots, n_1,\ k = 1, \ldots, n_2\}$$

defines a basis for $\mathcal{O}_K$ [46, p. 48]. We conclude using the fact that

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1\omega_i\omega_j\alpha_2\omega'_k\omega'_l) = \mathrm{Tr}_{K_1/\mathbb{Q}}(\alpha_1\omega_i\omega_j)\mathrm{Tr}_{K_2/\mathbb{Q}}(\alpha_2\omega'_k\omega'_l)$$

□

The lattice generator matrix can be immediately obtained as the tensor product of the generator matrices $R^{(j)}$ corresponding to the forms $\mathrm{Tr}(\alpha_j xy)$, for $j = 1, \ldots, N$

$$R = R^{(1)} \otimes \cdots \otimes R^{(N)}.$$

The above generalizes the cyclotomic construction to $\mathbb{Q}(\zeta_m)$, where m is a square-free product of primes. We are now able to construct rotated $\mathbb{Z}^n$–lattices in other dimensions such as $n = 10, 12, 16, 22, 24, 27, 28, \ldots$.

Summarizing all the constructions seen so far, we notice that we get lattice codes in most dimensions. For example, the missing dimensions below 30 are

(1) Some prime dimensions: $7, 13, 17, 19$. These can be obtained using *cyclic constructions* which are available for all prime dimensions, [4].
(2) The cases $n = 4$ and $n = 25$ can be obtained combining two suitable rotated $\mathbb{Z}^n$–lattices of dimension 2, respectively 5, [4].

Concerning the minimum product distance for the mixed construction, we have the following:

Proposition 7.4. [4] Let $K = K_1K_2$ be the compositum of two cyclotomic fields of degree n_1 and n_2, with coprime discriminant. The discriminant of K is $d_K = d_{K_1}^{m_1} d_{K_2}^{m_2}$, where $m_j = [K : K_j] = n/n_j$, $j = 1, 2$.

n	$d_{p,min}$	$\sqrt[n]{d_{p,min}}$	n	$d_{p,min}$	$\sqrt[n]{d_{p,min}}$
6	$1/\sqrt{5^3 7^4}$	0.349589	22	$1/\sqrt{5^{11}23^{20}}$	0.160801
10	$1/\sqrt{5^5 11^8}$	0.256271	24	$1/\sqrt{7^{16}17^{21}}$	0.151348
12	$1/\sqrt{5^6 13^{10}}$	0.229675	27	$1/\sqrt{7^{18}19^{24}}$	0.141242
15	$1/\sqrt{7^{10}11^{12}}$	0.200328	28	$1/\sqrt{5^{14}29^{26}}$	0.140051
16	$1/\sqrt{5^8 17^{14}}$	0.193613	30	$1/\sqrt{11^{24}13^{25}}$	0.131613
18	$1/\sqrt{5^9 19^{16}}$	0.180685			

Table 7.2 Minimum product distances for the mixed constructions.

As a direct consequence, we have that for the mixed construction

$$d_{p,min} = \frac{1}{\sqrt{d_{K_1}^{m_1} d_{K_2}^{m_2}}}.$$

Numerical values for $d_{p,min}$ are given in Table 7.2. Note that we also give the $d_{p,min}$ in some dimensions already available using the cyclotomic construction. The mixed construction yields a higher $d_{p,min}$ only for $n = 6$, but in general it is worse.

Remark 7.1. Another family of lattice codes has been found by what has been called *Krüskemper method* [39]. This approach allows us to maximize the minimum product distance and thus to improve the performance in dimensions where the other constructions yield a poor $d_{p,min}$ (see Fig. 7.3).

7.4 A Bound on Performance

The upper bound on the error probability (see Section 2.3) shows that we need to take into account both the diversity and the minimum product distance. Since maximal diversity is guaranteed using totally real number fields, we focus on the minimum product distance. The aim is to figure out what would be the maximal minimum product distance attained by ideal lattices [6]. By Theorem 6.1, $d_{p,min}$ only depends on d_K, the discriminant of K, so that we can use *Odlyzko's bound*. Odlyzko derived lower bounds for the *root discriminant* $d_K^{1/n}$

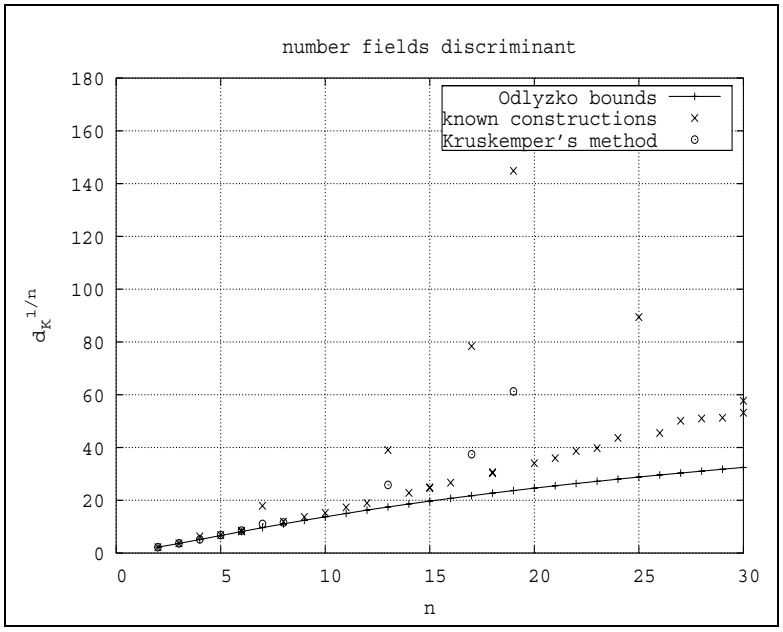

Fig. 7.3 Odlyzko bounds.

[38]. Asymptotically, we have the following behavior:

$$d_K^{1/n} \geq (60.8395...)^{r_1/n}(22.3816...)^{2r_2/n} - O(n^{-2/3}). \qquad (7.8)$$

Bounds for lower dimensions, which are of interest, are given in analytic form, but are hard to evaluate. Tables containing these values are available (see for example [2]). In Fig. 7.3, we compare the discriminant of known constructions [4, 39] to Odlyzko's bounds. This obviously yields an upper bound on the minimum product distance

$$d_{p,min}^{1/n} = (\frac{1}{\sqrt{d_K}})^{1/n} \leq \frac{1}{\sqrt{C_n}}$$

where C_n denotes Odlyzko's bound on the root discriminant in dimension n. In Figure 7.3, we observe that the discriminants of known constructions are close to the bounds, except for dimensions 7, 13, 17, 19 and 25. However, we show that even in the worst cases, they are good enough in the sense that any improvement would bring a negligible coding gain. We recall from [18] that the asymptotic coding gain

n	γ (dB)
7	0.03
13	0.09
17	0.12
19	0.21
25	0.25

Table 7.3 Some values of γ in dB relative to the bound.

between two rotated lattice constellations with the same dimension and maximal diversity is given by

$$\gamma = 10 \log_{10} \left(\frac{d_{p,min}(1)}{d_{p,min}(2)} \right)^{1/n} \quad [\text{dB}] \tag{7.9}$$

where $d_{p,min}(i)$, $i = 1, 2$ is the minimum product distance of each constellation. We compute the achievable coding gain obtained by using a number field whose discriminant would reach Odlyzko's bound, relatively to the given constructions. We observe in Table 7.3 that the maximal gain would be at most 0.25 dB.

Finally, we observe that $d_{p,min}^{1/n}$ decreases with n, suggesting that it vanishes asymptotically.

7.5 Some Simulation Results

A rotated $\mathbb{Z}^n$–lattice with diversity L is obtained by applying the rotation matrix M to the integer grid $\mathbb{Z}^n$, i.e.

$$\Lambda = \{\mathbf{x} = \mathbf{u}M, \ \mathbf{u} \in \mathbb{Z}^n\}.$$

The finite signal constellation is carved from this lattice by restricting the elements of $\mathbf{u}$ to a finite set of integers such as $\{\pm 1, \pm 3, \ldots \pm (2^{\eta/2} - 1)\}$, where η is the spectral efficiency measured in bits per two dimensions.

The newly constructed rotated $\mathbb{Z}^n$–lattice constellations have been simulated over an independent Rayleigh fading channel as defined in Section 2.

Figures 7.4 and 7.5 show the bit error rates of the rotated $\mathbb{Z}^n$ constellations for $\eta = 2, 4$ bit/symbol for the cyclotomic constructions. The

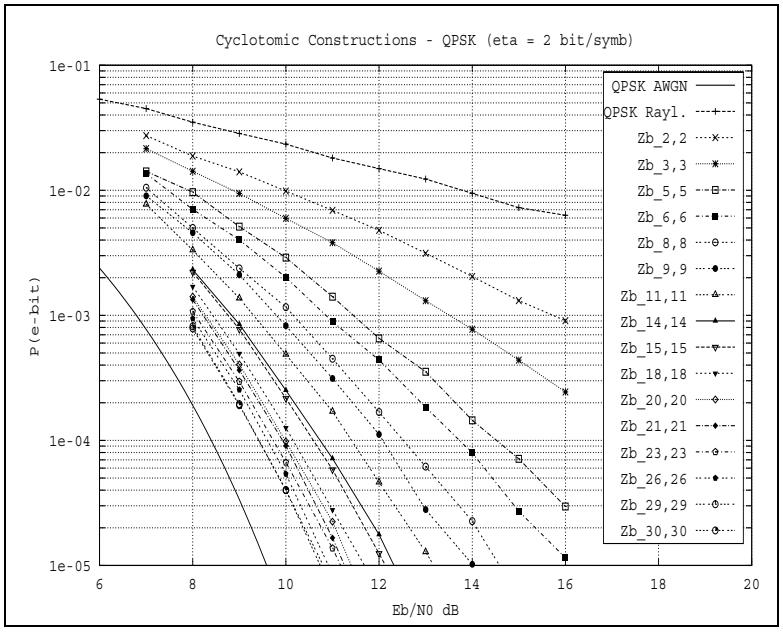

Fig. 7.4 Cyclotomic construction with QPSK.

rotated $\mathbb{Z}^n$ constellations are denoted by $\mathbb{Z}_{n,L}$, where the two subscripts indicate dimension and diversity. For comparison, the performance of a standard component interleaved QPSK (resp. 16-QAM) over Gaussian and Rayleigh fading channels is reported in the figures.

We can observe how the bit error rate performance over the Rayleigh fading channel approaches the one over the Gaussian channel as the diversity increases. Clearly, this gain is obtained at the expense of a higher decoding complexity due to the greater lattice dimension [52], but no extra bandwidth is used.

7.6 Appendix: Programming the Lattice Codes

We give KASH/KANT commands to compute the codes explained in this section.

The worked out example

We recall the beginning of the example, which has already been

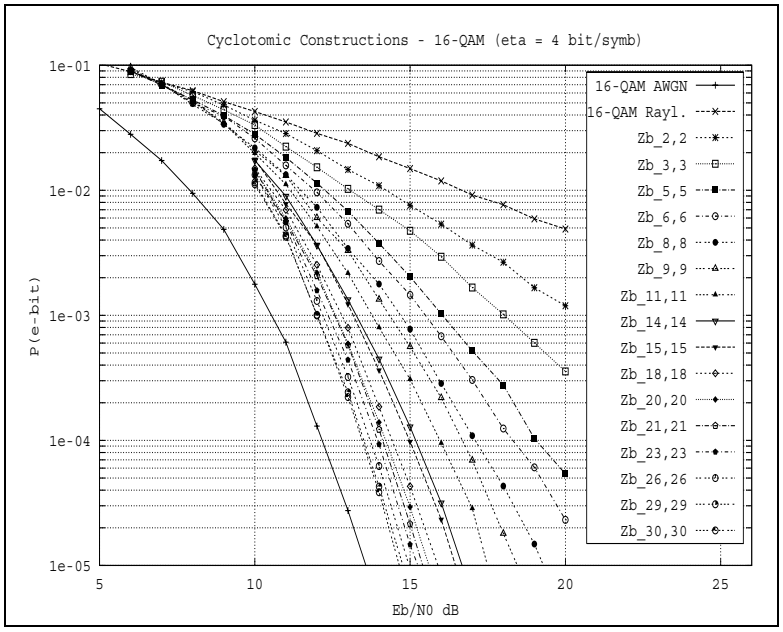

Fig. 7.5 Cyclotomic construction with 16-QAM.

explained in 5.5.

```
#compute the ring of integers
kash> O5:=OrderMaximal(Poly(Zx,[1,1,-1]));
Generating polynomial: x^2 + x - 1
Discriminant: 5

# ask for an integral basis
kash> B5:=OrderBasis(O5);
[ 1, [0, 1] ]
```

Recall that the integral basis is given in a $\mathbb{Q}$-basis $\{x, y\}$, that is $[a, b] = ax + by$, where $[0, 1]$ denotes a root of the minimal polynomial.

```
#generate alpha
kash> alpha:=Elt(O5,[2,-1]);
[2, -1]
```

```
#check the norm
kash> EltNorm(alpha);
5

#compute the embeddings
kash> OrderAutomorphisms(O5);
[ [0, 1], [-1, -1] ]
```

We now compute the generator matrix of the lattice. The command `EltAutomorphism` computes the conjugates of an element, while the command `EltCon` embeds an algebraic element into the real numbers.

```
# compute the lattice generator matrix
kash> M:= Mat(C,[[Sqrt(EltCon(alpha,1)),
                  Sqrt(EltCon(EltAutomorphism(alpha,2),1))],
                 [Sqrt(EltCon(alpha,1))*EltCon(1+B5[2],1),
                  Sqrt(EltCon(EltAutomorphism(alpha,2),1))
                  *EltCon(EltAutomorphism(1+B5[2],2),1)]]);
[1.1755705045 1.9021130325]
[1.9021130325 -1.1755705045]

#check the Gram matrix
kash> M*MatTrans(M);
[5.0000000000 -0.0000000000]
[-0.00000000  5]
```

We get indeed a scaled version of $\mathbb{Z}^2$, up to a scale factor 5.

The cyclotomic construction

We give here the commands in KASH/KANT. Note that this very short program, unlike the preceding examples, can be implemented in any language.

```
#initialization

p:=5;
n:=(p-1)/2;
```

```
sigma:=[];
l:=List([1..n],x->List([1..n],x->0));
M:=Mat(R,l);
T:=Mat(R,l);

zeta:= Exp(Comp(0,-2*pi/p));
alpha:=(1-zeta)*(1-zeta^(-1));

#compute sqrt(alpha_j)
for i in [1..n] do
    sigma[i]:= Sqrt(2-2*Cos(2*pi*i/p));
od;

#compute A
A:=MatDiag(R,sigma);

#compute M
for i in [1..n] do
    for j in [1..n] do
        M[i][j]:=2*Cos(2*pi*i*j/p);
    od;
od;

#compute T
for i in [1..n] do
    for j in [1..i] do
        T[i][j]:= 1;
    od;
od;

#compute R

G:= (1/Sqrt(p))*MatTrans(T)*M*A;
```

8

Other Applications and Conclusions

This work focuses on the application of algebraic number theory to code design for the single antenna Rayleigh fading channel. However, there are other contexts where these algebraic methods prove to be useful. In this last section, we give a brief overview of the following applications:

(1) dense lattices for the Gaussian channel
(2) complex lattices for the Rayleigh fading channel
(3) coherent MIMO channels.

Among these three topics, application to space–time coding is the most promising area for further research work. Recently, algebraic tools have been used to design space–time codes that have been shown to achieve the optimal diversity–multiplexing tradeoff.

8.1 Dense Lattices for the Gaussian Channel

When considering a Gaussian channel, the coding problem is equivalent to the *sphere packing problem*, i.e., how to pack together a large number of identical spheres as densely as possible (see Section 3.4). If

we are interested in increasing the coding gain over the Gaussian channel when transmitting lattice constellations, we need to consider dense lattices such as $D_4, E_6, E_7, E_8, K_{12}, \Lambda_{16}, \Lambda_{24}$ [23]. In order to simultaneously achieve some modulation diversity, we should construct these lattices algebraically. This approach was proposed in [18] and the algebraic constructions were given in [3]. Alternatively, we may use the fact that these lattices are sublattices of the rotated $\mathbb{Z}^n$–lattices to obtain maximal diversity.

8.2 Complex Lattices for the Rayleigh Fading Channel

In the single antenna Rayleigh fading channel considered in this work, we assume that the fading coefficients are real. This assumption is based on the use of an I/Q component interleaving that splits the complex fading coefficients. An alternative solution would be to assume complex fading, to avoid the use of the component interleaver. It appears that, in this case, all the theory explained about $\mathbb{Z}^n$ ideal lattices can be extended to the case of complex lattices.

Building $\mathbb{Z}^n$–lattices translates in the complex case to building $\mathbb{Z}[i]^n$ or $\mathbb{Z}[j]^n$–lattices. This leads to consider *relative* field extensions, that is field extensions of $\mathbb{Q}(i)$ or $\mathbb{Q}(j)$. The definition of ideal lattice can be naturally extended to this case, using a relative trace form. Similarly to the real case, we can define the diversity and the minimum product distance, and show that the latter is related to a field discriminant [5].

8.3 Space–Time Block Codes for the Coherent MIMO Channels

The purpose of this brief exposition is to give an example of such algebraic construction of a space–time block code.

One algebraic approach for building multi-antenna codes is based on *cyclic algebras* [44, 7]. The theory developed using non-commutative algebras to build coherent space–time block codes is beyond the scope of this work, so that we will restrict ourselves here to give an example to illustrate how the theory of algebraic lattices can be useful in this framework.

The example is a 2×2 full-rate space–time code called the *Golden code* [8]. We define the *infinite code* $\mathcal{C}_\infty$ as the set of matrices of the form

$$\mathcal{C}_\infty = \left\{ \mathbf{X} = \begin{bmatrix} a + b\theta & c + d\theta \\ i(c + d\bar{\theta}) & a + b\bar{\theta} \end{bmatrix} : a, b, c, d \in \mathbb{Z}[i] \right\}$$

where $\theta = \frac{1+\sqrt{5}}{2}$ and $\bar{\theta} = \frac{1-\sqrt{5}}{2}$. The *finite code* $\mathcal{C}$ is obtained by limiting the *information symbols* to $a, b, c, d \in S \subset \mathbb{Z}[i]$. In order to obtain *energy efficient* codes, we need to construct a lattice $M\mathbb{Z}[i]^2$, a rotated version of the complex lattice $\mathbb{Z}[i]^2$, where M is a complex unitary matrix, so that there is no shaping loss in the signal constellation emitted by the transmit antennas.

The complex lattice $M\mathbb{Z}[i]^2$ can be equivalently seen as a rotated $\mathbb{Z}^4$–lattice: $R\mathbb{Z}^4$, R being an orthogonal matrix, obtained from an ideal of $\mathcal{O}_L$, where $L = \mathbb{Q}(i, \theta)$. As seen previously in (6.4), a necessary condition to obtain $R\mathbb{Z}^4$ is that there exists an ideal $\mathcal{I} \subseteq \mathcal{O}_L$ such that its norm satisfies

$$N(\mathcal{I})^2 d_L = c^n, \ c \in \mathbb{Z} \ . \tag{8.1}$$

Since $d_L = 2^4 5^2$, we then need an ideal whose norm is 5. It can be shown that the principal ideal $\mathcal{I} = (\alpha)$, where $\alpha = 1 + i - i\theta$ has norm 5 and the resulting ideal lattice is indeed $\mathbb{Z}[i]^2$ as shown in [8]. We thus define our code $\mathcal{C}_\infty$ by restricting the codeword matrix entries to belong $\mathcal{I}$. Codewords of $\mathcal{C}_\infty$ are given by

$$\begin{aligned} \mathbf{X} &= \operatorname{diag}\left(M \begin{bmatrix} a \\ b \end{bmatrix} \right) + \operatorname{diag}\left(M \begin{bmatrix} c \\ d \end{bmatrix} \right) \cdot \begin{bmatrix} 0 & 1 \\ i & 0 \end{bmatrix} \\ &= \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha(a + b\theta) & \alpha(c + d\theta) \\ i\bar{\alpha}(c + d\bar{\theta}) & \bar{\alpha}(a + b\bar{\theta}) \end{bmatrix} \end{aligned}$$

where $a, b, c, d \in \mathbb{Z}[i]$, $\bar{\alpha} = 1 + i(1 - \bar{\theta})$ and the factor $\frac{1}{\sqrt{5}}$ is used to normalize M to a unitary matrix.

The determinants of the codewords are discrete, and the *minimum determinant* was shown to be $1/5$, which guarantees a non-vanishing determinant, whenever the size of the constellation increases. The additional property on the shape of the constellation obtained via the lattice was never considered before and appears to be the key factor to the improved performance of this code.

8.4 Conclusions

In this tutorial paper we have reviewed the basic concepts of algebraic number theory used to design codes for transmission over the Rayleigh fading channel. We have seen how this rich mathematical theory enables us to construct rotated $\mathbb{Z}^n$–lattice constellations with the desired modulation diversity and minimum product distance. We have shown how these properties are intimately related to the fundamental parameters of the underlying number fields. We strongly believe that algebraic number theory will have more applications to the design of signal space codes for various transmission systems.

References

[1] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, "Closest point search in lattices," *IEEE Transactions on Information Theory*, vol. 48, n. 8, pp. 2201–2214, 2002.

[2] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier, "PARI/GP – a software package for computer-aided number theory,". Available at http://www.math.u-psud.fr/~belabas/pari/.

[3] E. Bayer-Fluckiger, "Lattices and number fields," *Contemporary Mathematics*, vol. 241, pp. 69–84, 1999.

[4] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, "New algebraic constructions of rotated $\mathbb{Z}^n$–lattice constellations for the Rayleigh fading channel," *IEEE Transactions on Information Theory*, vol. 50, n. 4, pp. 702–714, 2004.

[5] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, "Algebraic lattice constellations: Bounds on performance," *submitted to IEEE Transactions on Information Theory*, April 2004.

[6] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, "Bounds on the performance of rotated lattice constellations," *Proceedings of the IEEE International Symposium on Information Theory*, April 2004.

[7] J.-C. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding," *Proceedings of ITW2003, Paris*, April 2003.

[8] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "The Golden code: A 2x2 full-rate space-time code with non-vanishing determinants," *Proceedings of the IEEE International Symposium on Information Theory*, 2004.

[9] K. Boullé and J.-C. Belfiore, "Modulation schemes designed for the Rayleigh channel," *Proc. CISS, Princeton, NJ*, pp. 288–293, 1992.

[10] J. Boutros, "Constellations optimales par plongement canonique," *Mémoire de fin d'études, E.N.S.T. Paris*, 1992.

[11] J. Boutros, "Réseaux de points pour les canaux à évanouissements," *Ph.D. thesis, E.N.S.T. Paris*, 1996.

[12] J. Boutros and E. Viterbo, "High diversity lattices for fading channels," *Proceedings 1995 IEEE International Symposium on Information Theory*, 1995.

[13] J. Boutros and E. Viterbo, "New approach for transmission over fading channel," *Proceedings of ICUPC'96*, pp. 66–70, 1996.

[14] J. Boutros and E. Viterbo, "Number fields and modulations for the fading channel," *presented at the workshop Réseaux Euclidiens et Formes Modulaires, Colloque CIRM, Luminy*, 1996.

[15] J. Boutros and E. Viterbo, "Rotated multidimensional QAM constellations for Rayleigh fading channels," *Proceedings of the 1996 IEEE Information Theory Workshop*, 1996.

[16] J. Boutros and E. Viterbo, "Rotated trellis coded lattices," *Proceedings of the XXVth General Assembly of the International Union of Radio Science, URSI*, 1996.

[17] J. Boutros and E. Viterbo, "Signal Space Diversity: a power and bandwidth efficient diversity technique for the Rayleigh fading channel," *IEEE Transactions on Information Theory*, vol. 44, n. 4, pp. 1453–1467, 1998.

[18] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good lattice constellations for both Rayleigh fading and gaussian channels," *IEEE Transactions on Information Theory*, vol. 42, n. 2, pp. 502–518, 1996.

[19] J. Boutros and M. Yubero, "Converting the Rayleigh fading channel into a Gaussian channel," *Mediterranean Workshop on Coding and Information Integrity*, 1996.

[20] L. Brunel and J. Boutros, "Lattice decoding for joint detection in direct-sequence cdma systems," *IEEE Transactions on Information Theory*, pp. 1030–1037, 2003.

[21] H. Cohen, *A Course in Computational Algebraic Number Theory*. Springer-Verlag, 1993.

[22] H. Cohn, *Advanced Number Theory*. Dover Publications, New York, 1980.

[23] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*. Springer-Verlag, New York, 1988.

[24] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, and K. Wildanger, "Kant v4," *J. Symbolic Comp.*, vol. 24, pp. 267–283, 1997.

[25] M. O. Damen, A. Chkeif, and J.-C. Belfiore, "Lattice code decoder for space-time codes," *IEEE Communications Letters*, vol. 4, n. 5, pp. 161–163, 2000.

[26] M. O. Damen, H. El Gamal, and G. Caire, "On maximum-likelihood detection and the search for the closest lattice point," *IEEE Transactions on Information Theory*, vol. 49, n. 10, pp. 2389–2402, 2003.

[27] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Mathematics of Computation*, vol. 44, pp. 463–471, 1985.

[28] G. D. Forney Jr., "Multidimensional constellations. ii. Voronoi constellations," *IEEE Journal on Selected Areas in Communications*, vol. 7, n. 6, pp. 941–958, 1989.

[29] X. Giraud, "Constellations pour le canal à évanouissements," *Ph.D. thesis, E.N.S.T. Paris*, 1994.

[30] X. Giraud and J.-C. Belfiore, "Constellation design for Rayleigh fading channels," *Proceedings of the 1996 IEEE Information Theory Workshop*, p. 25, 1996.

[31] X. Giraud and J.-C. Belfiore, "Constellations matched to the Rayleigh fading channel," *IEEE Transactions on Information Theory*, vol. 42, n. 1, pp. 106–115, 1996.

[32] X. Giraud, K. Boullé, and J.-C. Belfiore, "Constellations designed for the Rayleigh fading channel," *Proceedings of ISIT'93*, p. 342, 1993.

[33] X. Giraud, E. Boutillon, and J.-C. Belfiore, "Algebraic tools to build modulation schemes for fading channels," *IEEE Transactions on Information Theory*, vol. 43, n. 3, pp. 938–952, 1997.

[34] Giraud, X. and Belfiore, J.-C., "Coset codes on constellations matched to the fading channel," *Proceedings of ISIT'94*, p. 26, 1994.

[35] B. Hassibi and H. Vikalo, "On the expected complexity of sphere decoding," *Thirty-Fifth Asilomar Conference on Signals, Systems and Computers*, vol. 2, n. 4-7, pp. 1051–1055, 2001.

[36] B. Jeličić and S. Roy, "Design of a trellis coded QAM for flat fading and AWGN channels," *IEEE Transactions on Vehicular Technology*, vol. 44, n. 1, 1995.

[37] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*. Cambridge University Press, 1994.

[38] Odlyzko, A. M., "Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results," *Séminaire de Théorie des Nombres, Bordeaux*, pp. 1–15, 1989.

[39] F. Oggier and E. Bayer-Fluckiger, "Best rotated cubic lattice constellations for the Rayleigh fading channel," *Proceedings of the IEEE International Symposium on Information Theory*, 2003.

[40] M. Pohst, "KASH/KANT-computer algebra system,". Technische Universität, Berlin, Available at http://www.math.tu-berlin.de/algebra/.

[41] M. Pohst, "On the computation of lattice vectors of minimal length, successive minima and reduced basis with applications," *ACM SIGSAM Bulletin*, vol. 15, pp. 37–44, 1981.

[42] M. Pohst, *Computational algebraic number theory*. DMV Seminar, vol. 21, Birkhäuser Verlag, 1993.

[43] P. Samuel, *Théorie Algébrique des Nombres*. Hermann, 1971.

[44] B. A. Sethuraman, B. Sundar Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Transactions on Information Theory*, vol. 49, n. 10, October 2003.

[45] I. N. Stewart and D. O. Tall, *Algebraic Number Theory*. Chapman and Hall, 1979.

[46] H. P. F. Swinnerton-Dyer, *A Brief Guide to Algebraic Number Theory*. University Press of Cambridge, 2001.

[47] G. Taricco and E. Viterbo, "Performance of component interleaved signal sets for fading channels," *Electronics Letters*, vol. 32, n. 13, pp. 1170–1172, October 1996.

[48] G. Taricco and E. Viterbo, "Performance of high diversity multidimensional constellations," *IEEE International Symposium on Information Theory*, October 1997.

[49] G. Taricco and E. Viterbo, "Performance of high diversity multidimensional constellations," *IEEE Transactions on Information Theory*, vol. 44, n. 4, pp. 1539–1543, July 1998.

[50] E. Viterbo, "Tecniche matematiche computazionali per l'analisi ed il progetto di costellazioni a reticolo," *Ph.D. thesis, Politecnico di Torino*, 1995.

[51] E. Viterbo and E. Biglieri, "A universal lattice decoder," 14^{eme} *Colloque GRETSI*, pp. 611–614, 1993.

[52] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Transactions on Information Theory*, vol. 45, n. 5, pp. 1639–1642, 1999.

[53] L. C. Washington, *Introduction to Cyclotomic Fields*. Springer-Verlag, NY, 1982.

[54] M. A. Yubero, "Réseaux de points à haute diversité," *Proyecto fin de carrera, Escuele Técnica Superior de Ingenieros de Telecomunicación, Madrid Spain*, 1995.